ON THE ELLIPTIC CURVE $y^2 = x(x^2 + p)$ OVER SOME CERTAIN IMAGINARY QUADRATIC FIELDS

XIUMEI LI

Abstract. In this paper, we will talk about the titled elliptic curve defined over imaginary quadratic fields such as $K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-q})$, where q is congruent to 3 modulo 8 and $(p, q) = 1$.

1. Introduction and Main Results

In this paper, we study the elliptic curve

$$E_p : y^2 = x(x^2 + p), \tag{1.1}$$

where p is any odd rational prime. A.Bremner in [1] studied the elliptic curve E_p defined over $\mathbb{Q}$, determined the Selmer groups, and also obtained some results on Mordell-Weil group, rank, Sharevich-Tate groups and torsion subgroups. A.Bremner and J.W.S.Cassels in [2] parameterized generators for the group of rational points on the elliptic curve $E_p/\mathbb{Q}$, when p is congruent to 5 modulo 8 and less than 1,000. In this paper, we study the elliptic curve E_p defined over $K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-7})$ or $\mathbb{Q}(\sqrt{-q})$, where q is congruent to 3 modulo 8 and $(p, q) = 1$.

For any odd rational prime p, it's easy to see that the discriminate Δ of the elliptic curve E_p/K is equal to -2^6p^3 and the equation (1.1) is global minimal.

We now introduce the Kodaria-Néron classification of the special fibers $\mathcal{C}_\iota$ on the Néron models of elliptic curves E_p/K. Let $\iota \in \mathbb{O}_K$ be a prime element which divides the rational prime l, K_ι be the completion of K at prime ι, $k_\iota = \mathbb{O}_K/\iota\mathbb{O}_K$ be the residue class field with characteristic l. Let $\rho : E_p(K_\iota) \longrightarrow \widetilde{E_p}(k_\iota)$, $P \mapsto \widetilde{P}$ be the reduction of E_p modulo ι, $\widetilde{E_{p,\mathrm{ns}}}(k_\iota)$ be the non-singular k_ι-rational points of $\widetilde{E_p}(k_\iota)$, $E_{p,0}(K_\iota) = \rho^{-1}(E_{p,\mathrm{ns}}(k_\iota))$. The Kodaira symbols $I_0, I_1, I_n, II, III, IV, \cdots, III^*, II^*$ are used to describe the type of the special fiber $\mathcal{C}_\iota$ of the minimal Néron model of E_p at ι; m_ι denotes the number of irreducible components (ignoring multiplicities) on the special fiber $\mathcal{C}_\iota$. The conductor of E_p/K is defined by $N_{E_p} = \prod \iota^{f(E_p/K_\iota)}$, where the product takes for ι running over prime elements. The index $c_\iota = |E_p(K_\iota)/E_{p,0}(K_\iota)|$ is said to be Tamagawa constant at prime ι. Using the Tate's algorithm in [8], we could obtain the following Theorem 1.1 for notations.

Theorem 1.1. *For any odd prime p, let E_p/K be the defined elliptic curve as (1.1), then*

Table : the local invariants of $E_p/\mathbb{Q}(\sqrt{-1})$

prime ι	*spec. cond.*	*Kod.*	m_ι	$v_\iota(f(E_p/K))$	*Tam. num.* c_ι	$v_\iota(\Delta_{min})$
$\iota \not| 2p$		I_0	1	0	1	0
$\iota \| 2$	$p \equiv 1 (\mathrm{mod}\ 4)$	I_0^*	5	8	2	12
	$p \equiv 3 (\mathrm{mod}\ 4)$	I_2^*	7	6	$3 + (-1)^{\frac{p+1}{4}}$	12
$\iota \| p$		III	2	2	2	3

Table : the local invariants of $E_p/\mathbb{Q}(\sqrt{-2})$

2000 *Mathematics Subject Classification.* Primary 14H52; Secondary 11G05.
Key words and phrases. elliptic curve, Selmer group, Mordell-Weil group.

prime ι	*spec. cond.*	*Kod.*	m_ι	$v_\iota(f_E)$	*Tam. num.* c_ι	$v_\iota(\Delta_{min})$
$\iota \not\mid 2p$		I_0	1	0	1	0
$\iota \mid 2$	$p \equiv 1 (\mathrm{mod}\ 4)$	III^*	8	5	2	12
	$p \equiv 3 (\mathrm{mod}\ 8)$	I_3^*	8	5	$3+(-1)^{\frac{p-3}{8}}$	12
	$p \equiv 7 (\mathrm{mod}\ 8)$	I_3^*	8	5	$3+(-1)^{\frac{p-7}{8}}$	12
$\iota \mid p$		III	2	2	2	3

Table : the local invariants of E_p/K*, where* $K = \mathbb{Q}(\sqrt{-7})$ *or* $\mathbb{Q}(\sqrt{-q})$ *with* $q \equiv 3 (\mathrm{mod}\ 8)$

prime ι	*spec. cond.*	*Kod.*	m_ι	$v_\iota(f_E)$	*Tam. num.* c_ι	$v_\iota(\Delta_{min})$
$\iota \not\mid 2p$		I_0	1	0	1	0
$\iota = 2$	$p \equiv 1 (\mathrm{mod}\ 4)$	II	1	6	1	6
	$p \equiv 3 (\mathrm{mod}\ 4)$	III	2	5	2	6
$\iota \mid p$		III	2	2	2	3

Our main results are to determine Selmer groups, Shafarevich-Tate group and Mordell-Weil group(for definitions and notations, see [7]). Take the following elliptic curve

$$E'_p : y^2 = x(x^2 - 4p). \tag{1.2}$$

be the 2-isogenous elliptic curve of E_p and

$$\phi : E_p \longrightarrow E'_p \text{ and } \widehat{\phi} : E'_p \longrightarrow E_p$$

be the corresponding 2-isogeny defined as

$$\phi((x,y)) = \left(\frac{y^2}{x^2}, \frac{y(p-x^2)}{x^2}\right) \quad \text{and} \quad \widehat{\phi}((x,y)) = \left(\frac{y^2}{4x^2}, -\frac{y(4p+x^2)}{8x^2}\right)$$

with kernel $E_p[\phi] = \{O,\ (0,0)\}$ and $E'_p[\widehat{\phi}] = \{O,\ (0,0)\}$, respectively.

For simplicity, we denote the dimension $\dim_2 V = \dim_{\mathbb{F}_2} V$ for a vector space V over the field $\mathbb{F}_2$ of two elements.

Theorem 1.2. *For any odd prime* p *and* $K = \mathbb{Q}(\sqrt{-1})$*, let* E_p/K *and* E'_p/K *be the elliptic curves as (1.1) and (1.2), then*

(a)

$$E_p(K)_{tors} \cong \mathbb{Z}/2\mathbb{Z}.$$

(b)

$$S^{(\widehat{\phi})}(E'_p/K) \cong S^{(\phi)}(E_p/K).$$

$$S^{(\phi)}(E_p/K) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{if } p \equiv 7, 11 (\mathrm{mod}\ 16) \\ (\mathbb{Z}/2\mathbb{Z})^2, & \text{if } p \equiv 3, 5, 13, 15 (\mathrm{mod}\ 16) \\ (\mathbb{Z}/2\mathbb{Z})^3, & \text{if } p \equiv 1, 9 (\mathrm{mod}\ 16). \end{cases}$$

(c)

$$r(E_p(K)) + 2\dim_2(TS(E_p/K)[\phi]) = \begin{cases} 0, & \text{if } p \equiv 7, 11 (\mathrm{mod}\ 16) \\ 2, & \text{if } p \equiv 3, 5, 13, 15 (\mathrm{mod}\ 16) \\ 4, & \text{if } p \equiv 1, 9 (\mathrm{mod}\ 16). \end{cases}$$

Theorem 1.3. *For any odd prime* p *and* $K = \mathbb{Q}(\sqrt{-2})$*, let* E_p/K *and* E'_p/K *be the elliptic curves as (1.1) and (1.2), then*

(a)

$$E_p(K)_{tors} \cong \mathbb{Z}/2\mathbb{Z}.$$

(b) *If* $p \equiv 5, 7 (\mathrm{mod}\ 8)$, *then*

$$S^{(\phi)}(E_p/K) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } p \equiv 7 (\mathrm{mod}\ 16) \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p \equiv 5, 13, 15 (\mathrm{mod}\ 16) \end{cases}$$

$$S^{(\widehat{\phi})}(E'_p/K) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } p \equiv 13 (\mathrm{mod}\ 16) \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p \equiv 5, 7, 15 (\mathrm{mod}\ 16). \end{cases}$$

$$1 - r(E_p/K) = \begin{cases} \dim(TS(E'_p/K)[2]), & \text{if } p \equiv 7 (\mathrm{mod}\ 16) \\ \dim(TS(E_p/K)[2]), & \text{if } p \equiv 13 (\mathrm{mod}\ 16). \end{cases}$$

(c) *If* $p \equiv 1, 3 (\mathrm{mod}\ 8)$, *then* p *must be the sum of squares of two integers such as* $p = s^2 + 2t^2$.

$$S^{(\phi)}(E_p/K) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } p \equiv 3 (\mathrm{mod}\ 8) \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p \equiv 1 (\mathrm{mod}\ 8) \text{ and } s \equiv 3, 5 (\mathrm{mod}\ 8) \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{if } p \equiv 1 (\mathrm{mod}\ 8) \text{ and } s \equiv 1, 7 (\mathrm{mod}\ 8) \end{cases}$$

$$S^{(\widehat{\phi})}(E'_p/K) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } \underline{p \equiv 3 (\mathrm{mod}\ 8) \text{ or } p \equiv 9 (\mathrm{mod}\ 16) \text{ and } s \equiv 3, 5 (\mathrm{mod}\ 8)} \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } \underline{p \equiv 1 (\mathrm{mod}\ 16) \text{ and } s \equiv 3, 5 (\mathrm{mod}\ 8)} \\ & \quad \underline{\text{or } p \equiv 9 (\mathrm{mod}\ 16) \text{ and } s \equiv 1, 7 (\mathrm{mod} 8)} \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{if } p \equiv 1 (\mathrm{mod} 16) \text{ and } s \equiv 1, 7 (\mathrm{mod} 8). \end{cases}$$

(d) *If* $p \equiv 3 (\mathrm{mod}\ 8)$, *then*

$$E_p(K) \cong \mathbb{Z}/2\mathbb{Z}.$$

Theorem 1.4. *For any odd prime* p *and* $K = \mathbb{Q}(\sqrt{-7})$, *let* E_p/K *and* E'_p/K *be the elliptic curves as (1.1) and (1.2), then*

(a) $$E_p(K)_{tors} \cong \mathbb{Z}/2\mathbb{Z}.$$

(b) *If* $(\frac{p}{7}) = -1$, *then*

(b.1) If $p \equiv 7, 11 (\mathrm{mod}\ 16)$ *,then*

$$S^{(\phi)}(E_p/K) \cong \mathbb{Z}/2\mathbb{Z}, \quad S^{(\widehat{\phi})}(E'_p/K) \cong (\mathbb{Z}/2\mathbb{Z})^2,$$

$$r(E_p) + \dim TS(E'_p/K)[2] = 1.$$

(b.2) If $p \equiv 3, 5, 13 (\mathrm{mod}\ 16)$ *,then*

$$S^{(\phi)}(E_p/K) \cong (\mathbb{Z}/2\mathbb{Z})^2, \quad S^{(\widehat{\phi})}(E'_p/K) \cong \mathbb{Z}/2\mathbb{Z},$$

$$r(E_p/K) + \dim TS(E_p/K)[2] = 1.$$

(b.3) If $p \equiv 1 (\mathrm{mod}\ 8)$ *,then*

$$S^{(\phi)}(E_p/K) \cong (\mathbb{Z}/2\mathbb{Z})^4, \quad S^{(\widehat{\phi})}(E'_p/K) \cong \mathbb{Z}/2\mathbb{Z},$$

$$r(E_p/K) + \dim TS(E_p/K)[2] = 3.$$

(b.4) If $p \equiv 15 (\mathrm{mod}\ 16)$ *,then*

$$S^{(\phi)}(E_p/K) \cong (\mathbb{Z}/2\mathbb{Z})^3, \quad S^{(\widehat{\phi})}(E'_p/K) \cong (\mathbb{Z}/2\mathbb{Z})^2,$$

$$r(E_p/K) + \dim TS(E_p/K)[\phi] + \dim TS(E'_p/K)[\widehat{\phi}] = 3.$$

(c) *If* $(\frac{p}{7})=1$, *then* p *must be the quadratic form of two integers such as* $p=s^2-st+2t^2$. *Then*
(c.1) If $p\equiv 7,11(\text{mod } 16)$ *,then*

$$S^{(\phi)}(E_p/K)\cong\mathbb{Z}/2\mathbb{Z},\quad S^{(\widehat{\phi})}(E'_p/K)\cong(\mathbb{Z}/2\mathbb{Z})^2,$$
$$r(E_p/K)+\dim TS(E'_p/K)[2]=1.$$

(c.2) If $p\equiv 1(\text{mod } 8), s\equiv 3,5(\text{mod } 8)$ *and* $(\frac{2s-t}{7})=(-1)^{\frac{s+1}{2}}$, *then*

$$S^{(\phi)}(E_p/K)\cong(\mathbb{Z}/2\mathbb{Z})^3,\quad S^{(\widehat{\phi})}(E'_p/K)\cong\mathbb{Z}/2\mathbb{Z},$$
$$r(E_p/K)+\dim TS(E_p/K)[2]=2.$$

(c.3) If p *satisfies one of the following conditions: (c.3.1)* $p\equiv 3(\text{mod } 16)$ *and* $(\frac{2s-t}{7})=(-1)^{\frac{(s+2)^2-1}{8}}$; *(c.3.2)* $p\equiv 5(\text{mod } 8)$ *and* $(\frac{2s-t}{7})=(-1)^{\frac{s+1}{2}}$; *(c.3.3)* $p\equiv 15(\text{mod } 16)$ *and* $s\equiv 1,7(\text{mod } 8)$, *then*

$$S^{(\phi)}(E_p/K)\cong(\mathbb{Z}/2\mathbb{Z})^2,\quad S^{(\widehat{\phi})}(E'_p/K)\cong\mathbb{Z}/2\mathbb{Z},$$
$$r(E_p/K)+\dim TS(E_p/K)[2]=1.$$

(c.4) If p *satisfies one of the following conditions: (c.4.1)* $p\equiv 1(\text{mod } 8), s\equiv 3,5(\text{mod } 8)$ *and* $(\frac{2s-t}{7})=(-1)^{\frac{s-1}{2}}$; *(c.4.2)* $p\equiv 1(\text{mod } 8), s\equiv 1,7(\text{mod } 8)$ *and* $(\frac{2s-t}{7})=(-1)^{\frac{s+1}{2}}$, *then*

$$S^{(\phi)}(E_p/K)\cong(\mathbb{Z}/2\mathbb{Z})^4,\quad S^{(\widehat{\phi})}(E'_p/K)\cong\mathbb{Z}/2\mathbb{Z},$$
$$r(E_p/K)+\dim TS(E_p/K)[2]=3.$$

(c.5) If p *satisfies one of the following conditions: (c.5.1)* $p\equiv 3(\text{mod } 16)$ *and* $(\frac{2s-t}{7})=(-1)^{\frac{(s+2)^2+7}{8}}$; *(c.5.2)* $p\equiv 5(\text{mod } 8)$ *and* $(\frac{2s-t}{7})=(-1)^{\frac{s-1}{2}}$; *(c.5.3)* $p\equiv 15(\text{mod } 16)$ *and* $s\equiv 3,5(\text{mod } 8)$, *then*

$$S^{(\phi)}(E_p/K)\cong(\mathbb{Z}/2\mathbb{Z})^3,\quad S^{(\widehat{\phi})}(E'_p/K)\cong(\mathbb{Z}/2\mathbb{Z})^2,$$
$$r(E_p/K)+\dim TS(E_p/K)[\phi]+\dim TS(E'_p/K)[\widehat{\phi}]=3.$$

Theorem 1.5. *For any odd prime* p *and* $K=\mathbb{Q}(\sqrt{-q})$ *with* $q\equiv 3(\text{mod}8)$, *let* E_p/K *and* E'_p/K *be the elliptic curves as (1.1) and (1.2).*

(a) $E_p(K)_{tors}\cong\mathbb{Z}/2\mathbb{Z}$.

(b) *If* $(\frac{p}{q})=-1$, *then*

$$S^{(\phi)}(E_p/K)\cong\begin{cases}(\mathbb{Z}/2\mathbb{Z})^3, & \text{if } p\equiv 1(\text{mod } 8)\\ (\mathbb{Z}/2\mathbb{Z})^2, & \text{if } p\equiv 3,5,7(\text{mod } 8)\end{cases}\quad S^{(\widehat{\phi})}(E'_p/K)\cong\begin{cases}\mathbb{Z}/2\mathbb{Z}, & \text{if } p\equiv 1(\text{mod } 4)\\ (\mathbb{Z}/2\mathbb{Z})^2, & \text{if } p\equiv 3(\text{mod } 4)\end{cases}$$

$$r(E_p/K)+\dim TS(E_p/K)[2]=\begin{cases}2, & \text{if } p\equiv 1(\text{mod } 8)\\ 1, & \text{if } p\equiv 5(\text{mod } 8).\end{cases}$$

$$r(E_p/K)+\dim TS(E_p/K)[\phi]+\dim TS(E'_p/K)[\widehat{\phi}]=2, \text{for } p\equiv 3(\text{mod } 4).$$

(c) *If* $(\frac{p}{q})=1$ *and* p *is the quadratic form of two integers such as* $p=s^2+st+\frac{1+q}{4}t^2$. *Then*

$$S^{(\phi)}(E_p/K)\cong\begin{cases}(\mathbb{Z}/2\mathbb{Z})^2, & \text{if } \underline{p\equiv 3(\text{mod } 4)} \text{ or } \underline{p\equiv 5(\text{mod } 8) \text{ and } (\frac{2s+t}{p})=-1}\\ (\mathbb{Z}/2\mathbb{Z})^3, & \text{if } \underline{p\equiv 1(\text{mod } 4) \text{ and } (\frac{2s+t}{p})=(-1)^{\frac{p+3}{4}}}\\ (\mathbb{Z}/2\mathbb{Z})^4, & \text{if } \underline{p\equiv 1(\text{mod } 8) \text{ and } (\frac{2s+t}{p})=1.}\end{cases}$$

$$S^{(\widehat{\phi})}(E'_p/K)\cong\begin{cases}\mathbb{Z}/2\mathbb{Z}, & \text{if } \underline{p\equiv 5(\text{mod } 8)} \text{ or } \underline{p\equiv 1(\text{mod}8) \text{ and } (\frac{2s+t}{p})=-1}\\ (\mathbb{Z}/2\mathbb{Z})^2, & \text{if } \underline{p\equiv 3(\text{mod } 4)} \text{ or } \underline{p\equiv 1(\text{mod}8) \text{ and } (\frac{2s+t}{p})=1.}\end{cases}$$

$$r(E_p/K) + \dim TS(E_p/K)[2] = \begin{cases} 2, & \text{if } p \equiv 1 (\text{mod } 4) \text{ and } (\frac{2s+t}{p}) = (-1)^{\frac{p+3}{4}} \\ 1, & \text{if } p \equiv 5 (\text{mod } 8) \text{ and } (\frac{2s+t}{p}) = -1. \end{cases}$$

Definition 1.6. Let E be an elliptic curve over number field L, the L-series of E/L is defined by

$$L(E/L, s) := \prod_{\mathcal{B}|N_E} (1 - a_{\mathcal{B}} N(\mathcal{B})^{-s} + N(\mathcal{B})^{1-2s})^{-1} \prod_{\mathcal{B}|N_E} (1 - a_{\mathcal{B}} N(\mathcal{B})^{-s})^{-1}, \ s \in \mathbb{C},$$

where $\mathcal{B}$ run over all prime ideals in $\mathbb{O}_L$,$a_{\mathcal{B}}$ is equal to $N(\mathcal{B}) + 1 - \mid \widetilde{E}(k_{\mathcal{B}}) \mid$ and $N(\cdot)$ is the absolute norm of ideals for $L/\mathbb{Q}$.

For $L = \mathbb{Q}(\sqrt{-1})$, the L-series $L(E_p/\mathbb{Q}(\sqrt{-1}), s)$ of the elliptic curve $E_p/\mathbb{Q}(\sqrt{-1})$ has the following property.

Theorem 1.7. *For any odd prime p, let $E_p/\mathbb{Q}(\sqrt{-1})$ be the defined elliptic curve as (1.1), then*

$$L(E_p/\mathbb{Q}(\sqrt{-1}), s) = L(E_p/\mathbb{Q}, s)^2.$$

This paper is organized as follows. In section 2 we calculate the torsion subgroup of the Mordell-Weil group $E_p(K)$. In section 3 we determine the Selmer groups $S^{(\phi)}(E_p/K)$ and $S^{(\hat{\phi})}(E'_p/K)$ of these elliptic curves E_p and their isogenous curves E'_p. In section 4 we prove our main results.

2. Computation of the Torsion groups

In this section, we determine the torsion subgroup $E_p(K)_{tors}$ of the Mordell-Weil group $E_p(K)$.

The celebrating Mordell-Weil Theorem tells us that the group $E(L)$ is a finitely generated Abelian group, for any elliptic curve E defined over a number field L. When $L = \mathbb{Q}$, by Mazur Theorem, the torsion subgroup $E(\mathbb{Q})_{tors}$ is either cyclic of order m, where $1 \leq m \leq 10$ or $m = 12$, or of the form $\mathbb{Z}^2 \oplus \mathbb{Z}^{2m}$, where $1 \leq m \leq 4$. If L is a quadratic field, then the following theorem classifies the possible torsions.

Theorem 2.1. *(Kamienny, [3], Kenku and Momose, [4]). Let L be a quadratic field and E an elliptic curve over L. Then the torsion subgroup $E(L)_{tors}$ of $E(L)$ is isomorphic to one of the following 26 groups:*

$$\mathbb{Z}_m, \text{ for } 1 \leq m \leq 18, m \neq 17,$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_{2m}, \text{ for } 1 \leq m \leq 6,$$
$$\mathbb{Z}_3 \oplus \mathbb{Z}_{3m}, \text{ for } m = 1, 2,$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_4.$$

For the group $E_p(K)_{tors}$, using the theorem above, one can obtain the following theorem.

Theorem 2.2. *For each odd rational prime p and any quadratic field L, let E_p/L be the elliptic curve defined as (1.1). If $2p \not| D(L/\mathbb{Q})$ or $L = \mathbb{Q}(\sqrt{-d})$ with $d = 1, 2$. Then*

$$E(L)_{tors} \cong \mathbb{Z}/2\mathbb{Z}.$$

where $D(L/\mathbb{Q})$ is the fundamental discriminant of L.

Proof. Let $Q = (x(Q), y(Q))$ be a non-trivial torsion point of order n in $E_p(L)$. We prove that n is equal to 2 and $Q = (0, 0)$. It's easy to see that $n = 2$ implies that $Q = (0, 0)$ is the unique 2-torsion point. According to Theorem 2.1, $E_p(L)_{tors}$ must be isomorphic to one of the following 10 groups:

$$\mathbb{Z}_{2m} \text{ or } \mathbb{Z}_3 \oplus \mathbb{Z}_6, \text{ for } 1 \leq m \leq 9$$

Claim that n is not equal to 3. If $[3]Q = O$, then $x([2]Q) = x(Q)$. By the duplication formula $x([2]Q) = (\frac{x(Q)^2 - p}{2y(Q)})^2$, then $x(Q)$ is a root of the polynomial $3x^4 + 6px^2 - p^2 = 0$, which is impossible. Thus $E_p(L)_{tors}$ must be isomorphic to one of the following 6 groups:

$$\mathbb{Z}_{2m}, \text{ for } 1 \leq m \leq 9, 3 \not| m.$$

Claim that n is not equal to 4. If $[4]Q = O$, then $[2]Q = (0,0)$. By the duplication formula $x([2]Q) = (\frac{x(Q)^2-p}{2y(Q)})^2$, then $x(Q)^2 - p = 0$, which is also impossible. Thus $E_p(L)_{tors}$ must be isomorphic to one of the following 3 groups:

$$\mathbb{Z}_{2m}, \text{ for } m = 1, 5, 7.$$

Claim that n is not equal to 5. If $[5]Q = O$, then $x([4]Q) = x(Q)$ and $x([2]Q) \neq x(Q)$. Using the duplication formula, we get

$$x(Q) = x([4]Q) = (\frac{x([2]Q)^2 - p}{2y([2]Q)})^2.$$

Theorem 7.1 in [7] tells us that $x(Q), y(Q), x([2]Q), y([2]Q)$ are all algebraic integers, thus $x(Q) = u^2, x([2]Q) = v^2$ and satisfy $(v^4 - p)^2 = 4u^2v^2(v^4 + p)$, where $u, v \in \mathbb{O}_L - \{0\}$. Since the left hand of the equation above is a perfect square, then there is an integer $c \in \mathbb{O}_L$ such that

$$v^4 + p = c^2, \quad v^4 - p = 2uvc \tag{2.1}$$

Equations (2.1) imply that $v|p$. Furthermore, since $v_\wp(uv) = 0$ for any prime ideal $\wp|p$ and u, v are integral, we obtain that $v \in \mathbb{O}_L^*$. By the equations (2.1) above, we obtain two equalities as follows,

$$2p = c(c - 2uv), \quad 2 = c(c + 2uv) \tag{2.2}$$

If $2 \nmid D(L/\mathbb{Q})$, then equation 2.2 has no solution. If $L = \mathbb{Q}(\sqrt{-d})$ with $d = 1, 2$, we take $L = \mathbb{Q}(\sqrt{-1})$ for an example. Equation (2.2) implies that $c = (1+\sqrt{-1})vs$ with $s \in \mathbb{O}_L^*$. Therefore, we obtain the following two relationship

$$1 = v^2 s(\sqrt{-1}s + (1 + \sqrt{-1})u), \quad p = v^2 s(\sqrt{-1}s - (1 + \sqrt{-1})u)$$

which implies that $p+1 = 2\sqrt{-1}(vs)^2$, which is impossible, that is, Q can not be a 5-torsion point.

Claim that n is not equal to 7. It's similar to the case of $n \neq 5$.

As discussed above, we have shown that

$$E_p(L)_{tors} \cong \mathbb{Z}/2\mathbb{Z}.$$

□

3. Computation of the Selmer groups

In this section, we determine the Selmer groups $S^{(\phi)}(E_p/K)$ and $S^{(\widehat{\phi})}(E'_p/K)$ of these elliptic curves E_p and their isogenous curves E'_p defined as (1.1) and (1.2).

Let M_K be the set of all places of K. For each place $v \in M_K$, let K_v be the completion of K at v, and $\mathrm{ord}_v()$ be the corresponding normalized additive valuation, if v is finite.

Put $S = \{\infty\} \cup \{\text{primes in } K \text{ dividing } 2p\}$, and

$$K(S,2) = \{d \in K^*/K^{*2} : \ \mathrm{ord}_v(d) \equiv 0 (\mathrm{mod}\ 2) \ \text{ for all } \ v \notin S\}.$$

For each $d \in K(S,2)$, the corresponding homogenous space can be simplified to the following forms:

$$C_d : \ dW^2 = d^2 - 4pZ^4; \quad C'_d : \ dW^2 = d^2 + pZ^4.$$

According to Proposition 4.9 in [7], we have the following identifications:

$$\{1, -p\} \subseteq S^{(\phi)}(E_p/K) = \{d \in K(S,2) : \ C_d(K_v) \neq \emptyset \text{ for all } v \in S\},$$

$$\{1, p\} \subseteq S^{(\widehat{\phi})}(E'_p/K) = \{d \in K(S,2) : \ C'_d(K_v) \neq \emptyset \text{ for all } v \in S\}.$$

3.1. $K = \mathbb{Q}(\sqrt{-1})$. Note that 2 totally ramifies in K, we write $\pi_2 = 1 - i$, where i is equal to $\sqrt{-1}$. Here $S = \{\infty, \pi_2\} \cup \{\text{primes in } K \text{ dividing } p\}$.

Note that $4 = -\pi_2^4$, so for each $d \in K(S, 2)$, the corresponding homogenous space can be simplified to the following forms:

$$C_d, C_d' : \ dW^2 = d^2 + pZ^4.$$

Lemma 3.1. *For $C_i : iW^2 = -1 + pZ^4$, then $C_i(K_{\pi_2}) \neq \emptyset$ if and only if $p \equiv 1, 3, 9, 15 (\text{mod } 16)$, where K_{π_2} is the completion of K at place π_2.*

Proof. Let $f(Z, W) = iW^2 + 1 - pZ^4$, $g(Z_1, W_1; t) = iW_1^2 + \pi_2^{4t} - pZ_1^4$, where $t \in \mathbb{Z}_{\geq 1}$. Then $C_i : f(Z, W) = 0$.

(a) If $p \equiv 5, 7, 11, 13 (\text{mod } 16)$, by explicit calculation, we get

$$v_{\pi_2}(f(z, w)) \leq \begin{cases} 1, & \text{for any } v_{\pi_2}(w) = 0; \\ 6, & \text{for any } v_{\pi_2}(w) = 1; \\ 5, & \text{for any } v_{\pi_2}(w) \geq 2 \end{cases} \tag{3.1}$$

and $v_{\pi_2}(g(z_1, w_1; t)) = 1$ for any $(z_1, w_1) \in \mathbb{O}_{K_{\pi_2}}^{*2}$, then $C_i(K_{\pi_2}) = \emptyset$.

(b) If $p \equiv 1 (\text{mod } 8)$, the following table gives solutions (z, w) to the congruence

$$iW^2 = -1 + pZ^4 (\text{mod } \pi_2^9)$$

for each of the remaining values of $p (\text{mod } 32)$,

$p (\text{mod } 32)$	1	9	17	25
(z, w)	$(1 + \pi_2, 0)$	$(1 + \pi_2, \pi_2^3 + \pi_2^4)$	$(-3, 0)$	$(1, \pi_2^3)$

by Hensel's Lemma in [7], $f(z, w) = 0$ has a solution in $K_{\pi_2}^2$, that is, $C_i(K_{\pi_2}) \neq \emptyset$.

(c) If $p \equiv 3, 15 (\text{mod } 16)$, the following table gives solutions (z, w) to the congruence

$$iW^2 = -1 + pZ^4 (\text{mod } \pi_2^7)$$

for each of the remaining values of $p (\text{mod } 16)$,

$p (\text{mod } 16)$	3	15
(z, w)	$(1, \pi_2)$	$(1, \pi_2 + \pi_2^2)$

which implies that $C_i(K_{\pi_2}) \neq \emptyset$.

(a-c) imply that

$$C_i(K_{\pi_2}) \neq \emptyset \text{ if and only if } p \equiv 1, 3, 9, 15 (\text{mod } 8).$$

□

In the following subsection, we determine the Selmer group $S^{(\phi)}(E_p/K)$ according to the ideal decomposition of p in K.

3.1.1. *p inertia.* Assume that p inertia in K, then $p \equiv 3 (\text{mod } 4)$. In this case, $S = \{\infty, \pi_2, p\}$ and $K(S, 2) = < i, \pi_2, p >$.

Under this case, one can obtain the following lemma.

Lemma 3.2. (1) *For $d \in K(S, 2)$, if $\pi_2 \mid d$, then $d \notin S^{(\phi)}(E_p/K)$.*

(2) *$i \in S^{(\phi)}(E_p/K) \iff p \equiv 3, 15 (\text{mod } 16)$.*

Proof. (1) It follows directly by the valuation property.

(2) Let $f(Z,W) = iW^2 + 1 - pZ^4$, $g(Z_1, W_1; t) = iW_1^2 + \pi_2^{4t} - pZ_1^4$, where $t \in \mathbb{Z}_{\geq 1}$. Then $C_i : f(Z,W) = 0$.

(a) Lemma 3.1 tells us that $C_i(K_{\pi_2}) \neq \emptyset$ if and only if $p \equiv 3, 15 (\text{mod } 16)$.

(b) If $p \equiv 3(\text{mod}8)$, then $-2u^2 \equiv 1(\text{mod } p)$ for some integer u; If $p \equiv 7(\text{mod}8)$, then $2v^2 \equiv 1(\text{mod } p)$ for some integer v. The following table gives solutions (z,w) to the congruence

$$iW^2 = -1(\text{mod } p)$$

for each of the remaining values of $p(\text{mod } 8)$,

$p(\text{mod } 8)$	3	7
(z,w)	$(0, u(1-i))$	$(0, v(1-i))$

which implies that $C_i(K_p) \neq \emptyset$.

(a) and (b), together with the definition of $S^{(\phi)}(E_p/K)$, we have proven that

$$i \in S^{(\phi)}(E_p/K) \iff p \equiv 3, 15(\text{mod}16).$$

□

For the Selmer group $S^{(\phi)}(E_p/K)$, one can obtain the following theorem.

Theorem 3.3. *For any odd rational prime p with $p \equiv 3(\text{mod}4)$, then*

$$S^{(\phi)}(E_p/K) \cong \begin{cases} \{1, p\}, & \text{if } p \equiv 7, 11(\text{mod}16) \\ \{1, i, p, ip\}, & \text{if } p \equiv 3, 15(\text{mod}16). \end{cases}$$

Proof. It follows directly from Lemma 3.2. □

3.1.2. *p splits.* Assume that p splits completely in K, then $p \equiv 1(\text{mod } 4)$. Denote that $p = \mu \cdot \bar{\mu}$, where $\mu, \bar{\mu} \in \mathbb{Z}[\sqrt{-1}]$ are two conjugate irreducible elements, we write $\mu = s + t \cdot \sqrt{-1}$ for some integers s, t. In this case, $S = \{\infty, \pi_2, \mu, \bar{\mu}\}$ and $K(S,2) =< i, \pi_2, \mu, \bar{\mu} >$.

Lemma 3.4. *Let $q = u^2 + v^2$ be an odd prime, and suppose that u is odd. Then*

$$(\frac{u}{q}) = 1 \text{ and } (\frac{v}{q}) = (\frac{2}{q}).$$

Proof. It follows from Proposition 5.2 in [5]. □

Under this case, one can obtain the following lemma.

Lemma 3.5. (1) *For $d \in K(S,2)$, if $\pi_2 \mid d$, then $d \notin S^{(\phi)}(E_p/K)$.*

(2) *$i \in S^{(\phi)}(E_p/K)$ if and only if $p \equiv 1(\text{mod}8)$.*

(3) *$\mu \in S^{(\phi)}(E_p/K)$ if and only if $t \equiv 0(\text{mod } 4)$ or $s \equiv 0(\text{mod } 2)$.*

Proof. (1) It follows directly by the valuation property.

(2) Let $f(Z,W) = iW^2 + 1 - pZ^4$. Then $C_i : f(Z,W) = 0$.

(a) Lemma 3.1 tells us that $C_i(K_{\pi_2}) \neq \emptyset$ if and only if $p \equiv 1(\text{mod } 8)$.

(b) Prove that $C_i(K_\mu) \neq \emptyset$ if and only if $(\frac{st}{p}) = 1$. If $C_i(K_\mu) \neq \emptyset$, for any point $(z,w) \in C_i(K_\mu)$, then (z,w) satisfies $\sqrt{-1} \cdot w^2 \equiv -1(\text{mod } p)$. Note that $\mu = s + t \cdot \sqrt{-1}$, it follows that

$$w^2 \equiv st(\text{mod } p),$$

which implies that $(\frac{st}{p}) = 1$. On the other hand, if $(\frac{st}{p}) = 1$, then there exists an integer u such that $su^2 \equiv t(\text{ mod } p)$, hence $v_p(t \cdot f(0,u)) \geq 1 > 2v_p(t \cdot \frac{\partial}{\partial W} f(0,u))$, by Hensel's Lemma, $C_i(K_\mu) \neq \emptyset$.

(c) Prove that $C_i(K_{\bar{\mu}}) \neq \emptyset$ if and only if $(\frac{st}{p}) = 1$. The proof is similar to (b).

(a), (b) and (c) and Lemma 3.4 implies that

$$i \in S^{(\phi)}(E_p/K) \Longleftrightarrow p \equiv 1(\text{mod}8).$$

(3) Let $f(Z, W) = W^2 - \mu - \bar{\mu}Z^4$, $g(Z_1, W_1; t) = W_1^2 - \mu \cdot \pi_2^{4t} - \bar{\mu}Z_1^4$, where $t \in \mathbb{Z}_{\geq 1}$. Then $C_\mu : f(Z, W) = 0$.

(a) If $p \equiv 5(\text{ mod } 8)$ and $t \equiv 1, 2, 3(\text{ mod } 4)$, by explicit calculation, we get $v_{\pi_2}(f(z, w)) \leq 3$ and $v_{\pi_2}(g(z_1, w_1; t)) \leq 3$ for any $z_1, w, w_1 \in \mathbb{O}^*_{K_{\pi_2}}$, then $f(Z, W) = 0$ has no solution in $K^2_{\pi_2}$, that is, $C_\mu(K_{\pi_2} = \emptyset$.

(b) If $p \equiv 1(\text{mod } 8)$ and $t \equiv 0(\text{mod } 4)$, the following table gives solutions (z, w) to the congruence

$$W^2 = \mu + \bar{\mu}Z^4(\text{mod } \pi_2^5)$$

for each of the remaining values of $(s + t) \equiv 0(\text{mod } 8)$,

$(s+t)(\text{mod } 8)$	1	3	5	7
(z, w)	$(0, 1)$	$(\pi_2, 1 + \pi_2)$	$(\pi_2, 1)$	$(0, 1 + \pi_2)$

which implies that $C_\mu(K_{\pi_2}) \neq \emptyset$.

(c) If $p \equiv 1(\text{mod } 4)$ and $t \equiv 1(\text{mod } 2)$, the following table gives solutions (z, w) to the congruence

$$W^2 = \mu + \bar{\mu}Z^4(\text{mod } \pi_2^9)$$

for each of the remaining values of $s(\text{mod } 16)$,

$s(\text{mod } 16)$	0	2	4	6	8	10	12	14
(z, w)	$(1, 0)$	$(1, 2)$	$(1 + \pi_2^2, \pi_2^3)$	$(-3, \pi_2^2)$	$(1, -4)$	$(-3, 2)$	$(1 + \pi_2, \pi_2^3)$	$(1, \pi_2^2)$

which follows that $C_\mu(K_{\pi_2}) \neq \emptyset$.

(d) Prove that $C_\mu(K_\mu) \neq \emptyset$ if and only if $(\frac{2s}{p}) = 1$. If $C_\mu(K_\mu) \neq \emptyset$, for any point $(z, w) \in C_\mu(K_\mu)$, then (z, w) satisfies $w^2 \equiv \bar{\mu}(\text{mod } p)$. Note that $\mu = s + t \cdot \sqrt{-1}$ and $\mu + \bar{\mu} = 2s$, it follows that

$$w^2 \equiv 2sz^4(\text{mod } p),$$

which implies that $(\frac{2s}{p}) = 1$. On the other hand, if $(\frac{2s}{p}) = 1$, then there exists an integer u such that $u^2 \equiv 2s(\text{mod } p)$, hence $v_p(f(1, u)) \geq 1 > 2v_p(\frac{\partial}{\partial W}f(1, u))$, which implies that $C_\mu(K_\mu) \neq \emptyset$.

(e) Prove that $C_\mu(K_{\bar{\mu}}) \neq \emptyset$ if and only if $(\frac{2s}{p}) = 1$. The proof is similar to (c).

(a-e) and Lemma 3.4 imply that

$$\mu \in S^{(\phi)}(E_p/K) \Longleftrightarrow t \equiv 0(\text{mod } 4) \text{ or } s \equiv 0(\text{mod } 2).$$

□

For the Selmer group $S^{(\phi)}(E_p/K)$, one can obtain the following theorem.

Theorem 3.6. *For any odd rational prime p with $p \equiv 1(\text{mod}4)$, then*

$$S^{(\phi)}(E_p/K) \cong \begin{cases} \{1, \mu, \bar{\mu}, p\} \text{ or } \{1, i\mu, i\bar{\mu}, p\}, & \text{if } p \equiv 5(\text{mod}8) \\ \{1, i, \mu, \bar{\mu}, i\mu, i\bar{\mu}, p, ip\}, & \text{if } p \equiv 1(\text{mod}8) \end{cases}$$

where p is the product of two primes μ and $\bar{\mu}$.

Proof. It follows directly from Lemma 3.5. □

3.2. $K = \mathbb{Q}(\sqrt{-2})$**.** Note that 2 is totally ramified in K, denote that $\pi_2 = \sqrt{-2}$. Here $S = \{\infty, \pi_2\} \cup \{\text{primes in } K \text{ dividing } p\}$.

Note that $4 = \pi_2^4$, so for each $d \in K(S,2)$, the corresponding homogenous space can be simplified to the following forms:

$$C_d: \ dW^2 = d^2 - pZ^4; \quad C'_d: \ dW^2 = d^2 + pZ^4.$$

Lemma 3.7. *For $C_{-1}: -W^2 = 1 - pZ^4$, then $C_{-1}(K_{\pi_2}) \neq \emptyset$ if and only if $p \equiv 1, 5, 9, 11, 13, 15 (\mod 16)$.*

Proof. Let $f(Z,W) = W^2 + 1 - pZ^4$, $g(Z_1, W_1; t) = W_1^2 + \pi_2^{4t} - pZ_1^4$, where $t \in \mathbb{Z}_{\geq 1}$. Then $C_{-1}: f(Z,W) = 0$.

(a) If $p \equiv 3, 7 (\mod 16)$, by explicit calculation, we get $v_{\pi_2}(f(z,w)) \leq 5$ and $v_{\pi_2}(g(z_1, w_1; t)) \leq 5$ for any $(z,w) \in \mathbb{O}^2_{K_{\pi_2}}, (z_1, w_1) \in \mathbb{O}^{*2}_{K_{\pi_2}}$, then $C_{-1}(K_{\pi_2}) = \emptyset$.

(b) The following table gives solutions (z,w) to the congruence

$$-W^2 = 1 - pZ^4 (\mod \pi_2^9)$$

for each of the remaining values of $p (\mod 32)$,

$p (\mod 32)$	1	5	9	11	13	15
(z,w)	$(1,0)$	$(1,-2)$	$(1,-2\pi_2)$	$(-1+\pi_2, -2+\pi_2)$	$(1-2\pi_2, -2(1+\pi_2))$	$(1,\pi_2)$
$p (\mod 32)$	17	21	25	27	29	31
(z,w)	$(5,0)$	$(5,-2)$	$(5,-2\pi_2)$	$(3+\pi_2, -2+\pi_2)$	$(5-2\pi_2, -2(1+\pi_2))$	$(5,\pi_2)$

by Hensel's Lemma in [7], $f(Z,W) = 0$ has a solution in $K^2_{\pi_2}$, that is, $C_{-1}(K_{\pi_2}) \neq \emptyset$.

(a) and (b) imply that

$$C_{-1}(K_{\pi_2}) \neq \emptyset \text{ if and only if } p \equiv 1, 5, 9, 11, 13, 15 (\mod 16).$$

□

Lemma 3.8. *For $C'_{-1}: -W^2 = 1 + pZ^4$, then $C'_{-1}(K_{\pi_2}) \neq \emptyset$ if and only if $p \equiv 1, 3, 5, 7, 11, 15 (\mod 16)$.*

Proof. It' similar to the proof of Lemma 3.7. □

In the following subsection, we determine the Selmer group $S^{(\phi)}(E_p/K)$ and $S^{(\hat{\phi})}(E'_p/K)$ according to the ideal decomposition of p in K.

3.2.1. *p inertia.* Assume that p inertia in K, then $p \equiv 5, 7 (\mod 8)$. In this case, $S = \{\infty, \pi_2, p\}$ and $K(S,2) =< i, \pi_2, p >$.

Under this case, one can obtain the following lemma.

Lemma 3.9. *For $C_{-1}: -W^2 = 1 - pZ^4$, then $C_{-1}(K_p) \neq \emptyset$.*

Proof. Let $f(Z,W) = iW^2 + 1 - pZ^4$. Then $C_{-1}: f(Z,W) = 0$. If $p \equiv 5 (\mod 8)$, then $-u^2 \equiv 1 (\mod p)$ for some integer u; If $p \equiv 7 (\mod 8)$, then $2v^2 \equiv 1 (\mod p)$ for some integer v.

As discussed above, the following table gives solutions (z,w) to the congruence

$$-W^2 = 1 (\mod p)$$

for each of the remaining values of $p (\mod 8)$,

$p (\mod 8)$	5	7
(z,w)	$(0,u)$	$(0, v\sqrt{-2})$

which implies that $C_{-1}(K_p) \neq \emptyset$. □

Lemma 3.10. *For $C'_{-1} : -W^2 = 1 + pZ^4$, then $C'_{-1}(K_p) \neq \emptyset$.*

Proof. It's similar to the proof of Lemma 3.9. □

For the Selmer group $S^{(\phi)}(E_p/K)$ and $S^{(\hat{\phi})}(E'_p/K)$, one can obtain the following theorem.

Theorem 3.11. *For any odd rational prime p with $p \equiv 5, 7 (\mathrm{mod} 8)$, then*

$$S^{(\phi)}(E_p/K) \cong \begin{cases} \{1, -p\}, & \text{if } p \equiv 7 (\mathrm{mod} 16) \\ \{\pm 1, \pm p\}, & \text{if } p \equiv 5, 13, 15 (\mathrm{mod} 16), \end{cases}$$

$$S^{(\widehat{\phi})}(E'_p/K) \cong \begin{cases} \{1, p\}, & \text{if } p \equiv 13 (\mathrm{mod} 16) \\ \{\pm 1, \pm p\}, & \text{if } p \equiv 5, 7, 15 (\mathrm{mod} 16). \end{cases}$$

Proof. It follows directly from Lemma 3.7, Lemma 3.8, Lemma 3.9 and Lemma 3.10. □

3.2.2. *p splits.* Assume that p splits completely in K, then $p \equiv 1, 3 (\mathrm{mod}\ 8)$. Denote that $p = \mu \cdot \overline{\mu}$, where $\mu, \overline{\mu} \in \mathbb{Z}[\sqrt{-2}]$ are two conjugate irreducible elements, we write $\mu = s + t \cdot \sqrt{-2}$ for some integers s, t. In this case, $S = \{\infty, \pi_2, \mu, \overline{\mu}\}$ and $K(S, 2) =< i, \pi_2, \mu, \overline{\mu} >$.

Lemma 3.12. *Let $q = u^2 + 2v^2$ be an odd prime. Then*

$$(\frac{u}{q}) = (-1)^{\frac{u-1}{2}\frac{q-1}{2}} (\frac{2}{u}),$$

where $(\frac{\cdot}{\cdot})$ is the Jacobi symbol.

Proof. It follows from quadratic reciprocity laws. □

Under this case, one can obtain the following lemma.

Proposition 3.13. (1) For $d \in K(S, 2)$, if $\pi_2 \mid d$, then $d \notin S^{(\phi)}(E_p/K)$.
(2) $-1 \in S^{(\phi)}(E_p/K)$ if and only if $p \equiv 1 (\mathrm{mod}\ 8)$.
(3) $\mu \in S^{(\phi)}(E_p/K)$ if and only if $p \equiv 1 (\mathrm{mod}\ 8)$ and $s \equiv 1, 7 (\mathrm{mod}\ 8)$.

Proof. (1) It follows directly by the valuation property.
(2) (a) Lemma 3.7 tells us that $C_{-1}(K_{\pi_2}) \neq \emptyset$ if and only if $p \equiv 1, 9, 11 (\mathrm{mod}\ 16)$.
(b) To prove that $C_{-1}(K_\mu) \neq \emptyset$ if and only if $p \equiv 1 (\mathrm{mod}\ 8)$. If $C_{-1}(K_\mu) \neq \emptyset$, for any point $(z, w) \in C_{-1}(K_\mu)$, then (z, w) satisfies $-w^2 \equiv 1 (\mathrm{mod}\ p)$, which implies that $p \equiv 1 (\mathrm{mod}\ 8)$. On the other hand, if $p \equiv 1 (\mathrm{mod}\ 8)$, then there exists an integer u such that $-u^2 \equiv 1 (\mathrm{mod}\ p)$, hence $v_p(f(0, u)) > 2v_p(\frac{\partial}{\partial W} f(0, u))$, by Hensel's Lemma, $C_{-1}(K_\mu) \neq \emptyset$.
(c) It's similar to prove that $C_{-1}(K_{\overline{\mu}}) \neq \emptyset$ if and only if $p \equiv 1 (\mathrm{mod}\ 8)$.
(a-c) and the definition of the Selmer group $S^{\phi}(E_p/K)$ imply that

$$-1 \in S^{(\phi)}(E_p/K) \Longleftrightarrow p \equiv 1 (\mathrm{mod}\ 8).$$

(3) Let $f(Z, W) = W^2 - \mu + \overline{\mu} Z^4, g(Z_1, W_1; l) = W_1^2 - \mu \pi_2^{4l} + \overline{\mu} Z_1^4$ with $l \in \mathbb{Z}_{\geq 1}$. Then $C_\mu : f(Z, W) = 0$.
(a) To prove that $C_\mu(K_\mu) \neq \emptyset$ if and only if $(\frac{-2s}{p}) = 1$. If $C_\mu(K_\mu) \neq \emptyset$, taking any point $(z, w) \in C_\mu(K_\mu)$, then $z = p^{-l} z_0$ and $w = p^{-2l} w_0$, where $v_p(w) = v_p(z) = 0, l \in \mathbb{Z}_{\geq 0}$ and satisfies $-W_0^2 \equiv 2sz_0^4 (\mathrm{mod}\ p)$, therefore, we have $(\frac{-2s}{p}) = 1$. On the other hand, if $(\frac{-2s}{p}) = 1$, there exists an integer a such that $-a^2 \equiv 2s (\mathrm{mod}\ p)$, then $v_p(f(1, a)) \geq 1 > 2v_p(f_W(1, a)) = 0$, by Hensel' Lemma, $C_\mu(K_\mu) \neq \emptyset$.
(b) It's similar to prove that $C_\mu(K_{\overline{\mu}}) \neq \emptyset$ if and only if $(\frac{2s}{p}) = 1$.

(c) If $p \equiv 1(\text{mod } 8)$, the following table gives solutions (z, w) and (z_1, w_1) to the congruences

$$-W^2 = -\mu + \overline{\mu} Z^4 (\text{mod } \pi_2^5) \text{ and } -W_1^2 = -\mu\pi_2^{4l} + \overline{\mu} Z_1^4 (\text{mod } \pi_2^5)$$

for each of the remaining values of $(s \text{ mod } 8, t \text{ mod } 4) = (\overline{s}, \overline{t})$,

$(\overline{s}, \overline{t})$	$(\overline{1}, \overline{0})$	$(\overline{5}, \overline{0})$	$(\overline{3}, \overline{2})$	$(\overline{7}, \overline{2})$
(z, w)	$(0, 1)$	$(\pi_2, 1)$	$(\pi_2, 1 + \pi_2)$	$(0, 1 + \pi_2)$
$(\overline{s}, \overline{t})$	$(\overline{1}, \overline{2})$	$(\overline{5}, \overline{2})$	$(\overline{3}, \overline{0})$	$(\overline{7}, \overline{0})$
$(z_1, w_1; l)$	$(1, 1 + \pi_2; \geq 2)$	$(1, 1 + \pi_2; 1)$	$(1, 1; 1)$	$(1, 1; \geq 2)$

which implies that $C_\mu(K_{\pi_2}) \neq \emptyset$.

(a-c) and Lemma 3.12 imply that

$$\mu \in S^{(\phi)}(E_p/K) \Longleftrightarrow p \equiv 1(\text{mod } 8) \text{ and } s \equiv 1, 7(\text{mod } 8).$$

□

Proposition 3.14. (1) For $d \in K(S, 2)$, if $\pi_2 \mid d$, then $d \notin S^{(\widehat{\phi})}(E'_p/K)$.

(2) $-1 \in S^{(\widehat{\phi})}(E'_p/K)$ if and only if $p \equiv 1(\text{mod } 16)$.

(3) $\mu \in S^{(\widehat{\phi})}(E'_p/K)$ if and only if $p \equiv 1(\text{mod } 16)$ and $s \equiv 1, 7(\text{mod } 8)$ or $p \equiv 9(\text{mod } 16)$ and $s \equiv 7(\text{mod } 8)$.

Proof. It's similar to the proof of Proposition 3.13. □

For the Selmer group $S^{(\phi)}(E_p/K)$ and $S^{(\widehat{\phi})}(E'_p/K)$, one can obtain the following theorem.

Theorem 3.15. *For any odd rational prime p with $p \equiv 1, 3(\text{mod } 8)$, then*

$$S^{(\phi)}(E_p/K) \cong \begin{cases} \{1, -p\}, & \text{if } p \equiv 3(\text{mod}8) \\ \{\pm 1, \pm p\}, & \text{if } p \equiv 1(\text{mod}8) \text{ and } s \equiv 3, 5(\text{mod } 8) \\ \{\pm 1, \pm p, \pm\mu, \pm\overline{\mu}\}, & \text{if } p \equiv 1(\text{mod}8) \text{ and } s \equiv 1, 7(\text{mod } 8) \end{cases}$$

$$S^{(\widehat{\phi})}(E'_p/K) \cong \begin{cases} \{1, p\}, & \text{if } p \equiv 3(\text{mod } 8) \\ \{1, p\}, & \text{if } p \equiv 9(\text{mod } 16) \text{ and } s \equiv 3, 5(\text{mod } 8) \\ \{\pm 1, \pm p\}, & \text{if } p \equiv 1(\text{mod}16) \text{ and } s \equiv 3, 5(\text{mod } 8) \\ \{1, p, \mu, \overline{\mu}\} \text{ or } \{1, p, -\mu, -\overline{\mu}\}, & \text{if } p \equiv 9(\text{mod } 16) \text{ and } s \equiv 1, 7(\text{mod } 8) \\ \{\pm 1, \pm p, \pm\mu, \pm\overline{\mu}\}, & \text{if } p \equiv 1(\text{mod}16) \text{ and } s \equiv 1, 7(\text{mod } 8) \end{cases}$$

where p is the product of two primes μ and $\overline{\mu}$.

Proof. It follows directly from Proposition 3.13 and Proposition 3.14. □

3.3. $K = \mathbb{Q}(\sqrt{-7})$. Note that 2 splits completely in K, denote that $\pi_2 = -\frac{1+\sqrt{-7}}{2}$, $\overline{\pi_2} = \frac{-1+\sqrt{-7}}{2}$. Here $S = \{\infty, \pi_2, \overline{\pi_2}\} \cup \{\text{primes in } K \text{ dividing } p\}$.

Lemma 3.16. *For $C_d : dW^2 = d^2 - 4pZ^4$, where $d = 2, \pi_2$. Then*

(1) *$C_d(K_{\pi_2}) \neq \emptyset$ if and only if $p \equiv 1, 9, 15(\text{mod } 16)$;*

(2) *$C_d(K_{\overline{\pi_2}}) \neq \emptyset$.*

Proof. We only take $d = \pi_2$ for an example. let $f(Z, W) = \pi_2 W^2 - 1 + (\bar{\pi_2})^2 pZ^4$, then $C_{\pi_2} : f(Z, W) = 0$.

(1) For necessity, note that $C_{\pi_2}(K_{\pi_2}) \neq \emptyset$ implies that $C_{\pi_2}(\mathbb{O}_{K_{\pi_2}}) \neq \emptyset$. Taking any point $(z, w) \in C_{\pi_2}(K_{\pi_2})$, where $z, w \in \mathbb{O}_{K_{\pi_2}}$ and satisfy $\pi_2 w^2 = 1 - (\bar{\pi_2})^2 p z^4$, taking the valuation mod 2^5 of both sides, we obtain the following three congruent equations:

$$0 \equiv 1 - (\overline{\pi_2})^2 p (\text{mod } 2^4); \pi_2 \equiv 1 - (\overline{\pi_2})^2 p (\text{mod } 2^4); 4\pi_2 \equiv 1 - (\overline{\pi_2})^2 p (\text{mod } 2^4),$$

which imply that $p \equiv 1, 9, 15$ (mod16). On the other hand, the following table gives solutions (z, w) to the congruence

$$\pi_2 W^2 = 1 - (\overline{\pi_2})^2 p Z^4 (\text{mod } 2^5)$$

for each of the remaining values of $p (\text{mod } 2^5)$,

$p (\text{mod } 2^5)$	1	9	15	17	25	31
(z, w)	$(1, 2)$	$(-1, 0)$	$(3, 1)$	$(3, 2)$	$(1, 0)$	$(1, 1)$

by Hensel's Lemma in [7], $f(z, w) = 0$ has a solution in $K_{\pi_2}^2$, that is, $C_{\pi_2}(K_{\pi_2}) \neq \emptyset$.

(2) Since $v_{\overline{\pi_2}}(f(1, 1)) > 2v_{\overline{\pi_2}}(f_W(1, 1))$, by Hensel's Lemma, we proved that $C_{\pi_2}(K_{\overline{\pi_2}}) \neq \emptyset$ for any odd prime p.

As discussed above, we have shown our lemma. □

Corollary 3.17. For $C_{\overline{\pi_2}} : \overline{\pi_2} W^2 = 1 - (\pi_2)^2 p Z^4$. Then

(1) $C_{\overline{\pi_2}}(K_{\overline{\pi_2}}) \neq \emptyset$ if and only if $p \equiv 1, 9, 15 (\text{mod } 16)$;
(2) $C_{\overline{\pi_2}}(K_{\pi_2}) \neq \emptyset$.

Proof. It's similar to the proof of Lemma 3.16. □

In the following subsection, we determine the Selmer group $S^{(\phi)}(E_p/K)$ and $S^{(\widehat{\phi})}(E'_p/K)$ according to the ideal decomposition of p in K.

3.3.1. *p inertia.* Assume that p inertia in K, then $\left(\frac{p}{7}\right) = -1$. Under the assumption above, here $S = \{\infty, \pi_2, \overline{\pi_2}, p\}$ and $K(S, 2) =< -1, \pi_2, \overline{\pi_2}, p >$.

Under this case, one can obtain the following lemma.

Proposition 3.18. (1) $-1 \in S^{(\phi)}(E_p/K) \iff p \equiv 1 (\text{mod } 4)$.

(2) (a) $2, \pi_2, \bar{\pi_2} \in S^{(\phi)}(E_p/K) \iff p \equiv 1, 9, 15 (\text{mod } 16)$.
(b) $-2 \in S^{(\phi)}(E_p/K) \iff p \equiv 1, 3, 9 (\text{mod } 16)$.
(c) $-\pi_2, -\bar{\pi_2} \in S^{(\phi)}(E_p/K) \iff p \equiv 1 (\text{mod } 8)$.

Proof. (1) It's similarly to the proof of Proposition 6.2 in [7].

(2) We only take $d = \pi_2$ for an example. let $f(Z, W) = \pi_2 W^2 - 1 + (\bar{\pi_2})^2 p Z^4$, then $C_d : f(Z, W) = 0$.

(i) Lemma 3.16 tells that $C_d(K_{\pi_2}) \neq \emptyset$ if and only if $p \equiv 1, 9, 15 (\text{mod } 16)$.

(ii) Lemma 3.16 tells that $C_d(K_{\overline{\pi_2}}) \neq \emptyset$.

(iii) If $p \equiv 1, 9, 15$ (mod 16), then there exists an integer a such that $a^2 \equiv 2 (\text{mod } p)$. By our assumption, $(\frac{-7}{p}) = -1$, we have $(\frac{-1-2a}{p})(\frac{-1+2a}{p}) = -1$. Without loss of generality, we may assume that $(\frac{-1+2a}{p}) = 1$, then $(-1 + 2a)b^2 \equiv 1 (\text{mod } p)$ for some $b \in \mathbb{Z}$. Taking $\alpha = \frac{b}{\pi_2}(a + \pi_2)$, then $v_p(f(0, \alpha)) > 2v_p(f_W(0, \alpha))$. By Hensel's Lemma, $C_d(K_p) \neq \emptyset$.

(i), (ii), (iii) and the definition of $S^{(\phi)}(E_p/K)$ imply that

$$\pi_2 \in S^{(\phi)}(E_p/K) \iff p \equiv 1, 9, 15 (\text{mod } 16).$$

□

Proposition 3.19. (1) For $d \in K(S,2)$, if one of the following conditions holds:
(a) $\pi_2 \mid d$; (b) $\overline{\pi_2} \mid d$. Then $d \notin S^{(\widehat{\phi})}(E'_p/K)$.
(2) $-1 \in S^{(\widehat{\phi})}(E'_p/K) \iff p \equiv 7, 11, 15 (\mathrm{mod}\ 16)$.

Proof. It's similar to the proof of Proposition 3.18. □

For the Selmer group $S^{(\phi)}(E_p/K)$ and $S^{(\widehat{\phi})}(E'_p/K)$, one can obtain the following theorem.

Theorem 3.20. *For any odd rational prime p with $(\frac{p}{7}) = -1$, then*

$$S^{(\phi)}(E_p/K) \cong \begin{cases} \{1, -p\} & \text{if } p \equiv 7, 11 (\mathrm{mod}\ 16) \\ \{1, -2, -p, 2p\} & \text{if } p \equiv 3 (\mathrm{mod}\ 16) \\ \{\pm 1, \pm p\} & \text{if } p \equiv 5 (\mathrm{mod}\ 8) \\ < \pi_2, \overline{\pi_2}, -p > & \text{if } p \equiv 15 (\mathrm{mod}\ 16) \\ < -1, \pi_2, \overline{\pi_2}, p > & \text{if } p \equiv 1 (\mathrm{mod}\ 8) \end{cases}$$

$$S^{(\widehat{\phi})}(E'_p/K) \cong \begin{cases} \{1, p\} & \text{if } p \equiv 1, 3, 5, 9, 13 (\mathrm{mod}\ 16) \\ \{\pm 1, \pm p\} & \text{if } p \equiv 7, 11, 15 (\mathrm{mod}\ 16) \end{cases}$$

Proof. It follows directly from Proposition 3.18 and Proposition 3.19. □

3.3.2. *p splits.* Assume that p splits completely in K, then $\left(\frac{p}{7}\right) = 1$. Denote that $p = \mu \cdot \bar{\mu}$, where $\mu = s + t\pi_2$ and $s, t \in \mathbb{Z}$. Here $S = \{\infty, \pi_2, \bar{\pi}_2, \mu, \bar{\mu}\}$ and $K(S,2) =< -1, \pi_2, \bar{\pi}_2, \mu, \bar{\mu} >$.

Lemma 3.21. *Let $q = u^2 - uv + 2v^2$ be an odd prime and suppose that $v = 2^r v'$, then*

$$\left(\frac{u-v}{q}\right) = (-1)^{\frac{u-1}{2}\cdot\frac{q-1}{2}}\left(\frac{-2}{q}\right)\left(\frac{2}{u}\right),$$

$$\left(\frac{u}{q}\right) = (-1)^{\frac{u-1}{2}\cdot\frac{q-1}{2}}\left(\frac{2}{u}\right),$$

$$\left(\frac{v}{q}\right) = (-1)^{\frac{v'-1}{2}\cdot\frac{q-1}{2}}\left(\frac{2^r}{q}\right).$$

$$\left(\frac{2u-v}{q}\right) = \begin{cases} \left(\frac{2u-v}{7}\right), & \text{if } r = 1 \\ (-1)^{\frac{u-1}{2}}\left(\frac{2u-v}{7}\right), & \text{if } r > 1 \end{cases}$$

where $(\frac{\cdot}{\cdot})$ is the Jacobi symbol.

Proof. It follows directly from quadratic reciprocity laws. □

Under this case, one can obtain the following proposition.

Proposition 3.22. (1) $-1 \in S^{(\phi)}(E_p/K)$ if and only if $p \equiv 1 (\mathrm{mod} 4)$.
(2) (a) $2 \in S^{(\phi)}(E_p/K)$ if and only if $p \equiv 1, 9, 15 (\mathrm{mod}\ 16)$.
(b) $-2 \in S^{(\phi)}(E_p/K)$ if and only if $p \equiv 1, 3, 9 (\mathrm{mod}\ 16)$.
(c) $\pi_2,\ \overline{\pi_2} \in S^{(\phi)}(E_p/K)$ if and only if $p \equiv 1 (\mathrm{mod}\ 8)$ and $s \equiv 1, 7 (\mathrm{mod}\ 8)$ or $p \equiv 15 (\mathrm{mod}\ 16)$ and $s \equiv 3, 5 (\mathrm{mod}\ 8)$
(d) $-\pi_2,\ -\overline{\pi_2} \in S^{(\phi)}(E_p/K)$ if and only if $p \equiv 1 (\mathrm{mod}\ 8)$ and $s \equiv 1, 7 (\mathrm{mod}\ 8)$.
(3) (a) $\mu \in S^{(\phi)}(E_p/K) \iff \begin{cases} p \equiv 1 (\mathrm{mod} 4) \\ \left(\frac{2s-t}{7}\right) = (-1)^{\frac{s-1}{2}}. \end{cases}$
(b) $\pi_2 \cdot \mu \in S^{(\phi)}(E_p/K) \iff \begin{cases} p \equiv 1 (\mathrm{mod} 8) \\ \left(\frac{2s-t}{7}\right) = \left(\frac{-2}{s}\right). \end{cases}$ or $\begin{cases} p \equiv 3 (\mathrm{mod} 16) \text{ and } s \equiv 3 (\mathrm{mod} 4) \\ \left(\frac{2s-t}{7}\right) = \left(\frac{2}{s}\right). \end{cases}$

$\overline{\pi_2} \cdot \mu \in S^{(\phi)}(E_p/K) \iff \begin{cases} p \equiv 1 (\mathrm{mod} 8) \\ \left(\frac{2s-t}{7}\right) = \left(\frac{-2}{s}\right). \end{cases}$

(c) $2\mu \in S^{(\phi)}(E_p/K) \iff \begin{cases} p \equiv 1 (\mathrm{mod}\ 8) \\ \left(\frac{2s-t}{7}\right) = (-1)^{\frac{s-1}{2}}. \end{cases}$

Proof. (1) It's similarly to the proof of Proposition 6.2 in [7].

(2) We only take $d = \pi_2$ for an example. let $f(Z, W) = \pi_2 W^2 - 1 + (\overline{\pi_2})^2 p Z^4$, then $C_{\pi_2} : f(Z, W) = 0$.

(a) Lemma 3.16 tells that $C_{\pi_2}(K_{\pi_2}) \neq \emptyset$ if and only if $p \equiv 1, 9, 15 (\text{mod } 16)$.

(b) Lemma 3.16 tells that $C_{\pi_2}(K_{\overline{\pi_2}}) \neq \emptyset$.

(c) To prove that $C_{\pi_2}(K_\mu) \neq \emptyset$ if and only if $(\frac{-st}{p}) = 1$. If $C_{\pi_2}(K_\mu) \neq \emptyset$, taking any point $(z, w) \in C_{\pi_2}(K_\mu)$, then (z, w) satisfies $-sw^2 \equiv t (\text{mod } p)$, which implies that $(\frac{-st}{p}) = 1$. On the other hand, if $(\frac{-st}{p}) = 1$, then there exists an integer u such that $-su^2 \equiv t (\text{mod } p)$, hence $v_p(t \cdot f(0, u)) > 2v_p(\frac{\partial}{\partial W}(t \cdot f(0, u)))$, by Hensel's Lemma, $C_{\pi_2}(K_\mu) \neq \emptyset$.

(d) It's similar to prove that $C_{\pi_2}(K_{\overline{\mu}}) \neq \emptyset$ if and only if $(\frac{t(s-t)}{p}) = 1$.

(a-d) and Lemma 3.21 imply that

$$\pi_2 \in S^{(\phi)}(E_p/K) \Leftrightarrow \underline{p \equiv 1(\text{mod } 8) \text{ and } s \equiv 1, 7(\text{mod } 8)}$$

$$\text{or } \underline{p \equiv 15(\text{mod } 16) \text{ and } s \equiv 3, 5(\text{mod } 8)}.$$

(3) We only take $d = \mu$ for an example. let $f(Z, W) = W^2 - \mu + 4\overline{\mu} Z^4, g(Z_1, W_1) = W_1^2 - \mu \cdot 2^{4l-2} + \overline{\mu} Z_1^4$, where $l \in \mathbb{Z}_{>0}$. Then $C_\mu : f(Z, W) = 0$.

(a) To prove that $C_\mu(K_\mu) \neq \emptyset$ if and only if $(\frac{-(2s-t)}{p}) = 1$. If $C_\mu(K_\mu) \neq \emptyset$, taking any point $(z, w) \in C_\mu(K_\mu)$, then (z, w) satisfies $W^2 \equiv -4(2s - t)z^4 (\text{mod } p)$ which implies that $(\frac{-(2s-t)}{p}) = 1$. On the other hand, if $(\frac{-(2s-t)}{p}) = 1$, there exists an integer u such that $u^2 \equiv -4(2s - t) (\text{mod } p)$, then $v_p(f(1, u)) > 2v_p(\frac{\partial}{\partial W}(f(1, u)))$, by Hensel' Lemma, $C_\mu(K_\mu) \neq \emptyset$.

(b) It's similar to prove that $C_\mu(K_{\overline{\mu}}) \neq \emptyset$ if and only if $(\frac{2s-t}{p}) = 1$.

(c) To prove that $p \equiv 1 (\text{mod } 4)$ implies that $C_\mu(K_{\pi_2}) \neq \emptyset$. If $p \equiv 1 (\text{mod } 4)$, the following table gives solutions (z, w) and (z_1, w_1) to the congruences

$$W^2 = \mu - 4\overline{\mu} Z^4 (\text{mod } 8) \text{ and } W_1^2 = \mu \cdot 2^{4l-2} - \overline{\mu} Z_1^4 (\text{mod } 8)$$

for each of the remaining values of $(s \text{ mod } 8, t \text{ mod } 8) = (\overline{s}, \overline{t})$,

$(\overline{s}, \overline{t})$	$(\overline{1}, \overline{0})$ or $(\overline{1}, \overline{4})$	$(\overline{5}, \overline{2})$ or $(\overline{5}, \overline{6})$	$(\overline{1}, \overline{2})$ or $(\overline{1}, \overline{6})$	$(\overline{5}, \overline{0})$ or $(\overline{5}, \overline{4})$
(z, w)	$(0, 1)$	$(0, 1)$	$(1, 1)$	$(1, 1)$
$(\overline{s}, \overline{t})$	$(\overline{3}, \overline{0})$	$(\overline{3}, \overline{4})$	$(\overline{7}, \overline{4})$	$(\overline{7}, \overline{0})$
$(z_1, w_1; l)$	$(1, 1; 1)$	$(1, 1; \geq 2)$	$(1, 1; 1)$	$(1, 1; \geq 2)$

which implies that $C_\mu(K_{\pi_2}) \neq \emptyset$.

(d) It's similar to prove that $p \equiv 1 (\text{mod } 4)$ implies that $C_\mu(K_{\overline{\pi_2}}) \neq \emptyset$.

(a-d) and Lemma 3.21 implies that

$$\mu \in S^{(\phi)}(E_p/K) \iff \begin{cases} p \equiv 1(\text{mod} 4) \\ (\frac{2s-t}{7}) = (-1)^{\frac{s-1}{2}}. \end{cases}$$

□

Proposition 3.23. (1) For $d \in K(S, 2)$, if one of the following conditions holds:

(a) $\pi_2 \mid d$; (b) $\overline{\pi_2} \mid d$; (c) $d = -1$. Then $d \notin S^{(\widehat{\phi})}(E'_p/K)$.

(2)

$$\mu \in S^{(\widehat{\phi})}(E'_p/K) \iff \begin{cases} \underline{p \equiv 7, 11 (\mathrm{mod} 16)} & \text{or } \underline{p \equiv 1 (\mathrm{mod} 8) \text{ and } s \equiv 1 (\mathrm{mod} 8)} \\ & \text{or } \underline{p \equiv 3 (\mathrm{mod} 16) \text{ and } s \equiv 5, 7 (\mathrm{mod} 8)} \\ & \text{or } \underline{p \equiv 5 (\mathrm{mod} 8) \text{ and } s \equiv 1 (\mathrm{mod} 4)} \\ & \text{or } \underline{p \equiv 15 (\mathrm{mod} 16) \text{ and } s \equiv 3, 5 (\mathrm{mod} 8)} \\ (\frac{2s-t}{7}) = 1. \end{cases}$$

Proof. It's similar to the proof of Proposition 3.22. □

For the Selmer group $S^{(\phi)}(E_p/K)$ and $S^{(\widehat{\phi})}(E'_p/K)$, one can obtain the following theorem.

Theorem 3.24. *For any odd rational prime p with $(\frac{p}{7}) = 1$, then*

$$S^{(\phi)}(E_p/K) \cong \begin{cases} \{1, -p\}, & \text{if } p \equiv 7, 11 (\mathrm{mod}\ 16) \\ < -2, -p >, & \text{if } p \equiv 3 (\mathrm{mod}\ 16) \text{ and } (\frac{2s-t}{7}) = -(\frac{-2}{s}) \\ < -1, p >, & \text{if } p \equiv 5 (\mathrm{mod}\ 8) \text{ and } (\frac{2s-t}{7}) = (-1)^{\frac{s+1}{2}} \\ < 2, -p >, & \text{if } p \equiv 15 (\mathrm{mod}\ 16) \text{ and } s \equiv 1, 7 (\mathrm{mod}\ 8) \\ < -1, 2, p >, & \text{if } p \equiv 1 (\mathrm{mod}\ 8) \text{ and } s \equiv 3, 5 (\mathrm{mod}\ 8) \\ & \quad \text{and } (\frac{2s-t}{7}) = (-1)^{\frac{s-1}{2}} \\ < -2, \pi_2\mu, -p > \text{ or } < -2, -\pi_2\mu, -p >, & \text{if } p \equiv 3 (\mathrm{mod}\ 16) \text{ and } (\frac{2s-t}{7}) = (\frac{-2}{s}) \\ < -1, \mu, -p >, & \text{if } p \equiv 5 (\mathrm{mod}\ 8) \text{ and } (\frac{2s-t}{7}) = (-1)^{\frac{s-1}{2}} \\ < \pi_2, \overline{\pi_2}, -p >, & \text{if } p \equiv 15 (\mathrm{mod}\ 16) \text{ and } s \equiv 3, 5 (\mathrm{mod}\ 8) \\ < -1, 2, \mu, \overline{\mu} >, & \text{if } p \equiv 1 (\mathrm{mod}\ 8) \text{ and } s \equiv 3, 5 (\mathrm{mod}\ 8) \\ & \quad \text{and } (\frac{2s-t}{7}) = (-1)^{\frac{s-1}{2}} \\ < -1, \pi_2, \overline{\pi_2}, p >, & \text{if } p \equiv 1 (\mathrm{mod}\ 8) \text{ and } s \equiv 1, 7 (\mathrm{mod}\ 8) \\ & \quad \text{and } (\frac{2s-t}{7}) = (-1)^{\frac{s+1}{2}} \\ < -1, \pi_2, \overline{\pi_2}, \mu, \overline{\mu} >, & \text{if } p \equiv 1 (\mathrm{mod}\ 8) \text{ and } s \equiv 1, 7 (\mathrm{mod}\ 8) \\ & \quad \text{and } (\frac{2s-t}{7}) = (-1)^{\frac{s-1}{2}} \end{cases}$$

$$S^{(\widehat{\phi})}(E'_p/K) \cong \begin{cases} \{1, p\}, & \text{if } p \equiv 1 (\mathrm{mod}\ 8) \text{ and } s \equiv 3, 5 (\mathrm{mod}\ 8) \\ \{1, p\}, & \text{if } p \equiv 1 (\mathrm{mod}\ 8) \text{ and } s \equiv 1, 7 (\mathrm{mod}\ 8) \\ & \quad \text{and } (\frac{2s-t}{7}) = (-1)^{\frac{s+1}{2}} \\ \{1, p\}, & \text{if } p \equiv 3 (\mathrm{mod}\ 16) \text{ and } (\frac{2s-t}{7}) = -(\frac{-2}{s}) \\ \{1, p\}, & \text{if } p \equiv 5 (\mathrm{mod}\ 8) \text{ and } (\frac{2s-t}{7}) = (-1)^{\frac{s+1}{2}} \\ \{1, p\}, & \text{if } p \equiv 15 (\mathrm{mod}\ 16) \text{ and } s \equiv 1, 7 (\mathrm{mod}\ 8) \\ \{1, p, \mu, \overline{\mu}\} \text{ or } \{1, p, -\mu, -\overline{\mu}\}, & \text{if } p \equiv 3 (\mathrm{mod}\ 16) \text{ and } (\frac{2s-t}{7}) = (\frac{-2}{s}) \\ \{1, p, \mu, \overline{\mu}\} \text{ or } \{1, p, -\mu, -\overline{\mu}\}, & \text{if } p \equiv 5 (\mathrm{mod}\ 8) \text{ and } (\frac{2s-t}{7}) = (-1)^{\frac{s-1}{2}} \\ \{1, p, \mu, \overline{\mu}\} \text{ or } \{1, p, -\mu, -\overline{\mu}\}, & \text{if } p \equiv 7, 11 (\mathrm{mod}\ 16) \\ \{1, p, \mu, \overline{\mu}\} \text{ or } \{1, p, -\mu, -\overline{\mu}\}, & \text{if } p \equiv 15 (\mathrm{mod}\ 16) \text{ and } s \equiv 3, 5 (\mathrm{mod}\ 8) \\ \{1, p, \mu, \overline{\mu}\} \text{ or } \{1, p, -\mu, -\overline{\mu}\}, & \text{if } p \equiv 1 (\mathrm{mod}\ 8) \text{ and } s \equiv 1, 7 (\mathrm{mod}\ 8) \\ & \quad \text{and } (\frac{2s-t}{7}) = (-1)^{\frac{s-1}{2}} \end{cases}$$

where p is the product of two primes μ and $\overline{\mu}$.

Proof. It follows directly from Proposition 3.22 and Proposition 3.23. □

3.4. $K = \mathbb{Q}(\sqrt{-q})$ **with** $q \equiv 3 (\mathrm{mod} 8)$**.** Note that 2 inertia in K, take $\{0, 1, \pi = \frac{1-\sqrt{-q}}{2}, -\overline{\pi}\}$ as the representative set of $\mathbb{O}_K/2\mathbb{O}_K$. Here $S = \{\infty, 2\} \cup \{\text{primes dividing } p\}$.

3.4.1. *p inertia.* Assume that p inertia in K, then $(\frac{p}{q}) = -1$. In this case, $S = \{\infty, 2, p\}$ and $K(S,2) =< -1, 2, p >$.

We have the following results:

Proposition 3.25. (1) $-1 \in S^{(\phi)}(E_p/K) \Longleftrightarrow p \equiv 1(\mathrm{mod}4)$.

(2) (a) $2 \in S^{(\phi)}(E_p/K) \iff p \equiv 1, 7(\mathrm{mod}8)$;

(b) $-2 \in S^{(\phi)}(E_p/K) \iff p \equiv 1, 3(\mathrm{mod}8)$.

Proof. (1) According to the proof of Proposition 6.2 in [7]. We only need to prove that: if $C_{-1}(K_2) \neq \emptyset$, then $p \equiv 1(\mathrm{mod}\ 4)$. If $C_{-1}(K_2) \neq \emptyset$, taking any point $(z, w) \in C_{-1}(K_2)$, then (z, w) satisfies the following equation

$$-w_0^2 = 2^{4l-2} - pz_0^4,$$

where $z = 2^{-l}z_0, w = 2^{-2l+1}w_0$ and $l \in \mathbb{Z}_{>0}$. It follows that $p \equiv 1(\mathrm{mod}\ 4)$.

(2) We only take $d = 2$ for an example. Let $f(Z, W) = 2W^2 + pZ^4 - 1$, then $C_2 : f(Z, W) = 0$. According to the proof of Proposition 6.2 in [7]. We only need to prove that $C_2(K_2) \neq \emptyset$ if and only if $p \equiv 1, 7(\mathrm{mod}8)$. If $C_2(K_2) \neq \emptyset$, taking any point $(z, w) \in C_2(K_2)$, then (z, w) satisfies the following congruent equation

$$2w^2 = 1 - pz^4,$$

where $v_2(z) = 0$ and $v_2(w) \geq 0$. If $v_2(w) = 0$, it follows that $p \equiv 7(\mathrm{mod}8)$; if $v_2(w) > 0$, it follows that $p \equiv 1(\mathrm{mod}8)$. On the other hand, the following table gives solutions (z, w) to the congruence

$$2W^2 = 1 - pZ^4(\mathrm{mod}\ 2^5)$$

for each of the remaining values of $p(\mathrm{mod}\ 2^5)$

$p(\mathrm{mod}\ 2^5)$	1	7	9	15	17	23	25	31
(z, w)	$(1, 0)$	$(3 + u, 1 + 2\pi + 2^2\pi)$	$(3, 2)$	$(1, 3)$	$(3, 0)$	$(3 + v, 1 + 2\pi + 2^2\pi)$	$(1, 2)$	$(1, 1)$

where $u = 2[1 + (-1)^{\frac{q-3}{8}}], v = 2[1 + (-1)^{\frac{q+5}{8}}]$.

By Hensel's Lemma, $f(z, w) = 0$ has a solution in K_2^2, which means that $C_2(K_2) \neq \emptyset$. □

Proposition 3.26. (1) For $d \in K(S,2)$, if $2 \mid d$, then $d \notin S^{(\widehat{\phi})}(E'_p/K)$.

(2) $-1 \in S^{(\hat{\phi})}(E'_p/K) \iff p \equiv 3(\mathrm{mod}\ 4)$.

Proof. It's similar to the proof of Proposition 3.25. □

For the Selmer group $S^{(\phi)}(E_p/K)$ and $S^{(\widehat{\phi})}(E'_p/K)$, one can obtain the following theorem.

Theorem 3.27. *For any odd rational prime p with $(\frac{p}{q}) = -1$, then*

$$S^{(\phi)}(E_p/K) \cong \begin{cases} < -1, 2, p > & \text{if } p \equiv 1(\mathrm{mod}\ 8) \\ < -2, -p > & \text{if } p \equiv 3(\mathrm{mod}\ 8) \\ < -1, p > & \text{if } p \equiv 5(\mathrm{mod}\ 8) \\ < 2, -p > & \text{if } p \equiv 7(\mathrm{mod}\ 8) \end{cases}$$

$$S^{(\widehat{\phi})}(E'_p/K) \cong \begin{cases} \{1, p\} & \text{if } p \equiv 1(\mathrm{mod}\ 4) \\ \{\pm 1, \pm p\} & \text{if } p \equiv 3(\mathrm{mod}\ 4) \end{cases}$$

Proof. It follows directly from Proposition 3.25 and Proposition 3.26. □

3.4.2. *p splits.* Assume that p splits completely in K, then $\left(\frac{p}{q}\right)=1$. Denote that $p=\mu\cdot\bar{\mu}$, where $\mu=s+t\pi$ and $s,t\in\mathbb{Z}$. Here $S=\{\infty,2,\mu,\bar{\mu}\}$ and $K(S,2)=<-1,2,\mu,\bar{\mu}>$.

We have the following results:

Proposition 3.28. (1) $-1\in S^{(\phi)}(E/K)\Longleftrightarrow p\equiv 1(\mathrm{mod}4)$.

(2) (a) $2\in S^{(\phi)}(E/K)\iff p\equiv 1,7(\mathrm{mod}8)$;

(b) $-2\in S^{(\phi)}(E/K)\iff p\equiv 1,3(\mathrm{mod}8)$.

(3) (a) $\mu\in S^{(\phi)}(E/K)\iff\begin{cases}p\equiv 1(\mathrm{mod}4)\\ (\frac{2s+t}{p})=1.\end{cases}$

(b) $2\mu\in S^{(\phi)}(E/K)\iff\begin{cases}p\equiv 1(\mathrm{mod}8)\\ (\frac{2s+t}{p})=1.\end{cases}$

Proof. (1) It's similarly to the proof of Proposition 6.2 in [7].

(2) It's similarly to the proof of Proposition 3.25.

(3) We only take $d=\mu$ for an example. let $f(Z,W)=W^2-\mu+4\overline{\mu}Z^4, g(Z_1,W_1)=W_1^2-\mu\cdot 2^{4l-2}+\overline{\mu}Z_1^4$, where $l\in\mathbb{Z}_{>0}$. Then $C_\mu: f(Z,W)=0$.

(i) To prove that $C_\mu(K_\mu)\neq\emptyset$ if and only if $(\frac{-(2s+t)}{p})=1$. If $C_\mu(K_\mu)\neq\emptyset$, taking any point $(z,w)\in C_\mu(K_\mu)$, then (z,w) satisfies $W^2\equiv -4(2s+t)z^4(\mathrm{mod}\ p)$ which implies that $(\frac{-(2s+t)}{p})=1$. On the other hand, if $(\frac{-(2s+t)}{p})=1$, there exists an integer u such that $u^2\equiv -4(2s+t)(\mathrm{mod}\ p)$, then $v_p(f(1,u))>2v_p(\frac{\partial}{\partial W}(f(1,u)))$, by Hensel' Lemma, $C_\mu(K_\mu)\neq\emptyset$.

(ii) It's similar to prove that $C_\mu(K_{\overline{\mu}})\neq\emptyset$ if and only if $(\frac{2s+t}{p})=1$.

(iii) To prove that $p\equiv 1(\mathrm{mod}\ 4)$ implies that $C_\mu(K_2)\neq\emptyset$. If $p\equiv 1(\mathrm{mod}\ 4)$, the following tables give solutions (z,w) and $(z_1,w_1;l)$ to the congruences

$$W^2=\mu-4\overline{\mu}Z^4(\mathrm{mod}\ 8)\ \text{and}\ W_1^2=\mu\cdot 2^{4l-2}-\overline{\mu}Z_1^4(\mathrm{mod}\ 8)$$

for each of the remaining values of $(s\ \mathrm{mod}\ 8, t\ \mathrm{mod}\ 8)=(\overline{s},\overline{t})$,

$$q\equiv 3(\mathrm{mod}\ 32)$$

$\overline{s}\setminus\overline{t}$	$\overline{0}$	$\overline{1}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{7}$
$\overline{0}$		$(1,1;\geq 2)$	$(-\overline{\pi},-\overline{\pi})$		$(1,\pi+2;\geq 2)$	$(-\overline{\pi}+2,\pi)$
$\overline{1}$	$(0,1)$		$(1,-\overline{\pi};1)$	$(\pi,1)$		$(1,-\overline{\pi};\geq 2)$
$\overline{3}$	$(1,1;1)$	$(1,\pi+2)$		$(\pi,-\overline{\pi}+2;1)$	(π,π)	
$\overline{4}$		$(1,\pi+2;1)$	$(-\overline{\pi},1)$		$(1,\pi;1)$	$(-\overline{\pi},\pi)$
$\overline{5}$	$(0,\pi)$		$(1,-\overline{\pi}+2;\geq 2)$	$(-\overline{\pi},1)$		$(1,-\overline{\pi}+2;1)$
$\overline{7}$	$(1,1;\geq 2)$	$(\pi,\pi+2)$		$(\pi,-\overline{\pi};1)$	$(1,\pi)$	

$$q\equiv 11(\mathrm{mod}\ 32)$$

$\overline{s}\setminus\overline{t}$	$\overline{0}$	$\overline{1}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{7}$
$\overline{1}$	$(0,1)$	$(-\overline{\pi},\pi)$		$(\pi,1)$	(π,π)	
$\overline{2}$		$(1,\pi;\geq 2)$	$(1,-\overline{\pi})$		$(\pi,1;\geq 2)$	$(\pi,-\overline{\pi})$
$\overline{3}$	$(1,1;1)$		$(1,-\overline{\pi};1)$	$(\pi,-\overline{\pi};1)$		$(1,-\overline{\pi};\geq 2)$
$\overline{5}$	$(1,1)$	$(0,\pi)$		$(-\overline{\pi},1)$	$(1,\pi)$	
$\overline{6}$		$(1,\pi+2;1)$	$(-\overline{\pi},-\overline{\pi})$		$(1,\pi;1)$	$(0,-\overline{\pi})$
$\overline{7}$	$(1,1;\geq 2)$		$(1,-\overline{\pi}+2;\geq 2)$	$(-\overline{\pi},\pi;1)$		$(1,-\overline{\pi}+2;1)$

$$q\equiv 19(\mathrm{mod}\ 32)$$

$\overline{s} \setminus \overline{t}$	$\overline{0}$	$\overline{1}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{7}$
$\overline{0}$		$(1, \pi + 2; 1)$	$(0, -\overline{\pi})$		$(1, \pi; 1)$	$(\pi, -\overline{\pi})$
$\overline{1}$	$(0, 1)$		$(1, -\overline{\pi} + 2; \geq 2)$	$(\pi, 1)$		$(1, -\overline{\pi} + 2; 1)$
$\overline{3}$	$(1, 1; 1)$	$(0, \pi)$		$(-\overline{\pi}, \pi; 1)$	$(1, \pi)$	
$\overline{4}$		$(1, \pi; \geq 2)$	$(-\overline{\pi}, -\overline{\pi})$		$(\pi, 1; \geq 2)$	$(0, -\overline{\pi})$
$\overline{5}$	$(1, 1)$		$(1, -\overline{\pi}; 1)$	$(-\overline{\pi}, 1)$		$(1, -\overline{\pi}; \geq 2)$
$\overline{7}$	$(1, 1; \geq 2)$	$(\overline{\pi}, \pi)$		$(\pi, -\overline{\pi}; 1)$	(π, π)	

$$q \equiv 27 (\text{mod } 32)$$

$\overline{s} \setminus \overline{t}$	$\overline{0}$	$\overline{1}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{7}$
$\overline{1}$	$(0, 1)$	$(0, \pi)$		$(\pi, 1)$	$(1, \pi)$	
$\overline{2}$		$(1, \pi + 2; 1)$	$(-\overline{\pi}, -\overline{\pi})$		$(1, \pi; 1)$	$(0, -\overline{\pi})$
$\overline{3}$	$(\pi, -\overline{\pi}; 1)$		$(1, -\overline{\pi} + 2; \geq 2)$	$(\pi, -\overline{\pi}; \geq 2)$		$(1, -\overline{\pi} + 2; 1)$
$\overline{5}$	$(1, 1)$	$(-\overline{\pi}, \pi)$		$(-\overline{\pi}, 1)$	(π, π)	
$\overline{6}$		$(1, \pi; \geq 2)$	$(1, -\overline{\pi})$		$(1, \pi + 2; \geq 2)$	$(\pi, -\overline{\pi})$
$\overline{7}$	$(\pi, -\overline{\pi} + 2; 1)$		$(1, -\overline{\pi}; 1)$	$(\pi, -\overline{\pi} + 2; \geq 2)$		$(1, -\overline{\pi}; \geq 2)$

which imply that $C_\mu(K_2) \neq \emptyset$.

(i),(ii) and (iii) imply that

$$\mu \in S^{(\phi)}(E_p/K) \iff \begin{cases} p \equiv 1 (\text{mod} 4) \\ (\frac{2s+t}{p}) = 1. \end{cases}$$

□

Proposition 3.29. (1) For $d \in K(S, 2)$, if one of the following conditions holds:

(a) $2 \mid d$; $(b) d = -1$. Then $d \notin S^{(\hat{\phi})}(E'_p/K)$.

(2)

$$\mu \in S^{(\overline{\phi})}(E'_p/K) \iff \begin{cases} p \equiv 3 (\text{mod} 4) \\ (\frac{2s+t}{p}) = 1. \end{cases}$$

$$\text{or} \begin{cases} p \equiv 1 (\text{mod } 8) \text{ and } s \equiv -\frac{q-3}{4} (\text{mod} 8) \text{ and } t \equiv 3 (\text{mod} 4) \\ (\frac{2s+t}{p}) = 1. \end{cases}$$

$$\text{or} \begin{cases} p \equiv 1 (\text{mod } 8) \text{ and } s - t \equiv -\frac{q-3}{4} + 6 (\text{mod} 8) \text{ and } t \equiv 1 (\text{mod} 4) \\ (\frac{2s+t}{p}) = 1. \end{cases}$$

$$\text{or} \begin{cases} p \equiv 1 (\text{mod } 8) \text{ and } s \equiv 1 (\text{mod } 4) \text{ and } t \equiv 0 (\text{mod } 8) \\ (\frac{2s+t}{p}) = 1. \end{cases}$$

Proof. It's similar to the proof of Proposition 3.28. □

For the Selmer group $S^{(\phi)}(E_p/K)$ and $S^{(\widehat{\phi})}(E'_p/K)$, one can obtain the following theorem.

Theorem 3.30. *For any odd rational prime p with $(\frac{p}{q}) = 1$, then*

$$S^{(\phi)}(E_p/K) \cong \begin{cases} \{1, -2, -p, 2p\}, & \text{if } p \equiv 3 (\text{mod } 8) \\ \{1, 2, -p, -2p\}, & \text{if } p \equiv 7 (\text{mod } 8) \\ \{1, -1, -p, p\}, & \text{if } p \equiv 5 (\text{mod } 8) \text{ and } (\frac{2s+t}{p}) = -1 \\ \{1, -1, \mu, -\mu, \overline{\mu}, -\overline{\mu}, p, -p\}, & \text{if } p \equiv 5 (\text{mod } 8) \text{ and } (\frac{2s+t}{p}) = 1 \\ \{1, -1, 2, -2, p, -p\}, & \text{if } p \equiv 1 (\text{mod } 8) \text{ and } (\frac{2s+t}{p}) = -1 \\ < -1, 2, \mu, \overline{\mu} >, & \text{if } p \equiv 1 (\text{mod } 8) \text{ and } (\frac{2s+t}{p}) = 1 \end{cases}$$

$$S^{(\widehat{\phi})}(E_p'/K) \cong \begin{cases} \{1,p\}, & \text{if } p \equiv 5(\text{mod } 8) \\ \{1,p\}, & \text{if } p \equiv 1(\text{mod } 8) \text{ and } (\frac{2s+t}{p}) = -1 \\ \{1,\mu,\overline{\mu},p\} \text{ or } \{1,-\mu,-\overline{\mu},p\}, & \text{if } p \equiv 3(\text{mod } 4) \\ \{1,\mu,\overline{\mu},p\} \text{ or } \{1,-\mu,-\overline{\mu},p\}, & \text{if } p \equiv 1(\text{mod } 8) \text{ and } (\frac{2s+t}{p}) = 1 \end{cases}$$

where p is the product of two primes μ and $\overline{\mu}$.

Proof. It follows directly from Proposition 3.28 and Proposition 3.29. □

4. The proof of the main results

Use the exact sequences listed in [7], we have

$$\begin{aligned} 0 &\longrightarrow \tfrac{E_p'(K)}{\phi(E_p(K))} \longrightarrow S^{(\phi)}(E_p/K) \longrightarrow \text{TS}(E_p/K)[\phi] \longrightarrow 0 \\ 0 &\longrightarrow \tfrac{E_p(K)}{\widehat{\phi}(E_p'(K))} \longrightarrow S^{(\widehat{\phi})}(E_p'/K) \longrightarrow \text{TS}(E_p'/K)[\widehat{\phi}] \longrightarrow 0 \\ 0 &\longrightarrow \tfrac{E_p'(K)[\widehat{\phi}]}{\phi(E_p(K)[2])} \longrightarrow \tfrac{E_p'(K)}{\phi(E_p(K))} \longrightarrow \tfrac{E_p(K)}{2E_p(K)} \longrightarrow \tfrac{E_p(K)}{\widehat{\phi}(E_p'(K))} \longrightarrow 0 \end{aligned}$$

which follows that

$$\begin{aligned} &\text{rank}(E_p/K) + \dim_2(\text{TS}(E_p/K)[\phi]) + \dim_2(\text{TS}(E_p'/K)[\widehat{\phi}]) \\ &= \dim_2(S^{(\phi)}(E_p/K)) + \dim_2(S^{(\widehat{\phi})}(E_p'/K)) - 2. \end{aligned} \tag{4.1}$$

Proof of Theorem 1.2. Theorem 3.3 and Theorem 3.6 tell us that

$$S^{(\phi)}(E_p/K) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{if } p \equiv 7,11(\text{mod}16) \\ (\mathbb{Z}/2\mathbb{Z})^2, & \text{if } p \equiv 3,5,13,15(\text{mod}16) \\ (\mathbb{Z}/2\mathbb{Z})^3, & \text{if } p \equiv 1,9(\text{mod}16) \end{cases}$$

Note that $\text{TS}(E_p/K)[\phi] \cong \text{TS}(E_p/K)[\hat{\phi}]$ and $S^{(\phi)}(E_p/K) \cong S^{(\hat{\phi})}(E_p'/K)$, together with equation (4.1) imply that

$$\text{rank}(E_p(K)) + 2\dim_2(\text{TS}(E_p/K)[\phi]) = 2\dim_2(S^{(\phi)}(E_p/K)) - 2.$$

As discussed above, one can obtain that

$$\text{rank}(E_p(K)) + 2\dim_2(\text{TS}(E_p/K)[\phi]) = \begin{cases} 0, & \text{if } p \equiv 7,11(\text{mod}16) \\ 2, & \text{if } p \equiv 3,5,13,15(\text{mod}16) \\ 4, & \text{if } p \equiv 1,9(\text{mod}16). \end{cases}$$

□

Proof of Theorem 1.3. If $p \equiv 5,7(\text{mod } 8)$, then theorem 3.11 tells us that

$$S^{(\phi)}(E_p/K) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } p \equiv 7(\text{mod } 16) \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p \equiv 5,13,15(\text{mod } 16) \end{cases}$$

$$S^{(\hat{\phi})}(E_p'/K) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } p \equiv 13(\text{mod } 16) \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p \equiv 5,7,15(\text{mod } 16). \end{cases}$$

If $p \equiv 1,3(\text{mod } 8)$, then theorem 3.15 tells us that

$$S^{(\phi)}(E_p/K) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } p \equiv 3(\text{mod } 8) \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p \equiv 1(\text{mod } 8) \text{ and } s \equiv 3,5(\text{mod } 8) \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{if } p \equiv 1(\text{mod } 8) \text{ and } s \equiv 1,7(\text{mod } 8) \end{cases}$$

$$S^{(\hat{\phi})}(E_p'/K) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } p \equiv 3(\text{mod } 8) \text{ or } p \equiv 9(\text{mod } 16) \text{ and } s \equiv 3,5(\text{mod } 8) \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p \equiv 1(\text{mod } 16) \text{ and } s \equiv 3,5(\text{mod } 8) \\ & \quad \text{or } p \equiv 9(\text{mod } 16) \text{ and } s \equiv 1,7(\text{mod}8) \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{if } p \equiv 1(\text{mod}16) \text{ and } s \equiv 1,7(\text{mod}8), \end{cases}$$

where p is equal to $s^2 + 2t^2$.

Equation (4.1) implies that $E_p(K) = \mathbb{Z}/2\mathbb{Z}$ for $p \equiv 3(\text{mod } 8)$ and

$$1 - r(E_p/K) = \begin{cases} \dim(\text{TS}(E'_p/K)[2]), & \text{if } p \equiv 7(\text{mod } 16) \\ \dim(\text{TS}(E_p/K)[2]), & \text{if } p \equiv 13(\text{mod } 16). \end{cases}$$

□

Proof of Theorem 1.4. It's similar to the proof of Theorem 1.2. □

Proof of Theorem 1.5. It's similar to the proof of Theorem 1.3. □

In the following subsection, we turn to show Theorem 1.7.

Proof of Theorem 1.7. This following is a list of lemmas as to the reduction of E_p.

Lemma 4.1. *Let l, p be any distinct odd primes and E_p be the elliptic curve over finite field $\mathbb{F}_l$ defined as (1.1), then l is supersingular if and only if $l \equiv 3(\text{mod } 4)$.*

Proof. It follows from Theorem 4.1 in [7]. □

Lemma 4.2. *Let l, p be any distinct odd primes and $E_p/\mathbb{F}_l$ be the elliptic curve defined as (1.1). If $E_p/\mathbb{F}_l$ is supersingular, then*

$$E_p(\mathbb{F}_{l^2}) \cong \mathbb{Z}/(l+1)\mathbb{Z} \oplus \mathbb{Z}/(l+1)\mathbb{Z}.$$

Proof. It follows from Lemma 4.1 and Theorem 4.1 in [9]. □

Lemma 4.3. *Let p be any odd prime and E_p/K be the elliptic curve defined as (1.1). For any rational prime l and prime π dividing l in $\mathbb{O}_K$, then*

$$a_\pi = \begin{cases} 0, & \text{if } \pi | 2p \\ a_l, & \text{if } l \nmid 2p \text{ and } l \equiv 1(\text{mod } 4) \\ -2l, & \text{if } l \nmid 2p \text{ and } l \equiv 3(\text{mod } 4). \end{cases}$$

Proof. According to the ideal decomposition of rational prime l in K, one can obtain that

$$k_\pi \cong \begin{cases} \mathbb{F}_2, & \text{if } l = 2 \\ \mathbb{F}_l, & \text{if } l \neq 2 \text{ and } l \equiv 1(\text{mod } 4) \\ \mathbb{F}_{l^2}, & \text{if } l \neq 2 \text{ and } l \equiv 3(\text{mod } 4). \end{cases}$$

The formula above and Lemma 4.2 imply that

$$|\widetilde{E_p}(k_\pi)| = \begin{cases} N(\pi) + 1, & \text{if } \pi | 2p \\ |\widetilde{E_p}(\mathbb{F}_l)|, & \text{if } l \nmid 2p \text{ and } l \equiv 1(\text{mod } 4) \\ (l+1)^2, & \text{if } l \nmid 2p \text{ and } l \equiv 3(\text{mod } 4). \end{cases}$$

As discussed above, the formula $a_\pi = N(\pi) + 1 - |\widetilde{E_p}(k_\pi)|$ implies that

$$a_\pi = \begin{cases} 0, & \text{if } \pi | 2p \\ a_l, & \text{if } l \nmid 2p \text{ and } l \equiv 1(\text{mod } 4) \\ -2l, & \text{if } l \nmid 2p \text{ and } l \equiv 3(\text{mod } 4). \end{cases}$$

□

Remark 4.4. When we consider E_p as the elliptic curve over the rational number field $\mathbb{Q}$, then

$$a_l = \begin{cases} 0, & \text{if } l | 2p \\ a_l, & \text{if } l \nmid 2p \text{ and } l \equiv 1(\text{mod } 4) \\ 0, & \text{if } l \nmid 2p \text{ and } l \equiv 3(\text{mod } 4), \end{cases}$$

which follows that

$$L(E_p/\mathbb{Q}, s) = \prod_{l \nmid 2p, l \equiv 1(\text{ mod } 4)} (1 - a_l l^{-s} + l^{1-2s})^{-1} \prod_{l \nmid 2p, l \equiv 3(\text{ mod } 4)} (1 + l^{1-2s})^{-1}.$$

By the definition of L-series $L(E_p/K,s)$ and ideal decomposition of rational prime, we have

$$L(E_p/K,s)=\prod_{\pi\nmid 2p}(1-a_\pi N(\pi)^{-s}+N(\pi)^{1-2s})^{-1}\prod_{\pi|2p}(1-a_\pi N(\pi)^{-s})^{-1}$$

$$=\prod_{l\nmid 2p,l\equiv 1(\bmod 4)}\prod_{\pi|l}(1-a_\pi N(\pi)^{-s}+N(\pi)^{1-2s})^{-1}\prod_{l\nmid 2p,l\equiv 3(\bmod 4)}\prod_{\pi|l}(1-a_\pi N(\pi)^{-s}+N(\pi)^{1-2s})^{-1}$$
$$\cdot\prod_{l=2}\prod_{\pi|2}(1-a_\pi N(\pi)^{-s})^{-1}\prod_{l=p}\prod_{\pi|p}(1-a_\pi N(\pi)^{-s})^{-1}.$$

On the other hand, Lemma 4.3 implies that

$$L(E_p/K,s)=\prod_{l\nmid 2p,l\equiv 1(\bmod 4)}(1-a_l l^{-s}+l^{1-2s})^{-2}\prod_{l\nmid 2p,l\equiv 3(\bmod 4)}(1+2l\cdot l^{-2s}+l^{2(1-2s)})^{-1}$$
$$=\prod_{l\nmid 2p,l\equiv 1(\bmod 4)}(1-a_l l^{-s}+l^{1-2s})^{-2}\prod_{l\nmid 2p,l\equiv 3(\bmod 4)}(1+l^{1-2s})^{-2}$$
$$=[\prod_{l\nmid 2p,l\equiv 1(\bmod 4)}(1-a_l l^{-s}+l^{1-2s})^{-1}\prod_{l\nmid 2p,l\equiv 3(\bmod 4)}(1+l^{1-2s})^{-1}\prod_{l=2}(1-2^{-s})^{-1}\prod_{l=p}(1-p^{-s})^{-1}]^2.$$

Note that

$$L(E_p/\mathbb{Q},s)=\prod_{l\nmid 2p,l\equiv 1(\bmod 4)}(1-a_l l^{-s}+l^{1-2s})^{-1}\prod_{l\nmid 2p,l\equiv 3(\bmod 4)}(1+l^{1-2s})^{-1},$$

which implies that

$$L(E_p/K,s)=L(E_p/\mathbb{Q},s)^2.$$

□

References

[1] A. Bremner, On the equation $y^2=x(x^2+p)$, in " Number Theory and Applications "(R.Mollin,ed.), Kluwer, Dordrecht, 3-23, 1989.

[2] A. Bremner and J.W.S.Cassels, On the equation $y^2=x(x^2+p)$, Math. Comp. 42, 1984, 257-264.

[3] S.Kamienny, Torsion points on elliptic curves and q-coefficients of modular forms, Invent. Math. 109, 1992, 221-229.

[4] M.A.Kenku and F.Momose, Torsion points on elliptic curves defined over quadratic fields, Nagoya Math.J.109,1988, 125-149.

[5] F. Lemmermeyer, Reciprocity Laws. From Euler to Eisenstein, Springer-Verlag Heidelberg, Springer Monographs in Mathematics.

[6] E.Selmer, A conjecute concerning rational points on cubic curves. Math. Scand. volume 2, 1954, pp.49-54.

[7] J.H.Silverman, The Arithmetic of Elliptic Curves, GTM 106, Springer-Verlag, New York, 1986.

[8] J.H. Silverman, Advances Topics in the Arithmetic of Elliptic Curves, Springer, New York, 1994.

[9] C.Wittmann, Group Structure of Elliptic Curves over Finite Fields, Journal of Number Theory 88, 2001, pp.335-344.

Department of Mathematical Science, Tsinghua University, Beijing, P. R. China 100084

E-mail address: xm-li09@mails.tsinghua.edu.cn